QSC 2021 VMDR

Qualys.

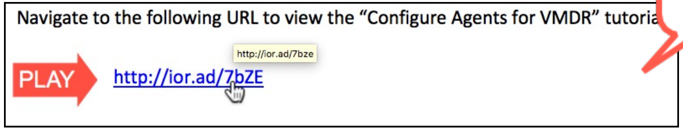
Course Training Documents

- QSC 2021 VMDR Lab Tutorial Supplement
- QSC 2021 VMDR Slides

You can download both documents from:

`https://bit.ly/qsc21vmdr`

Play Lab Tutorials

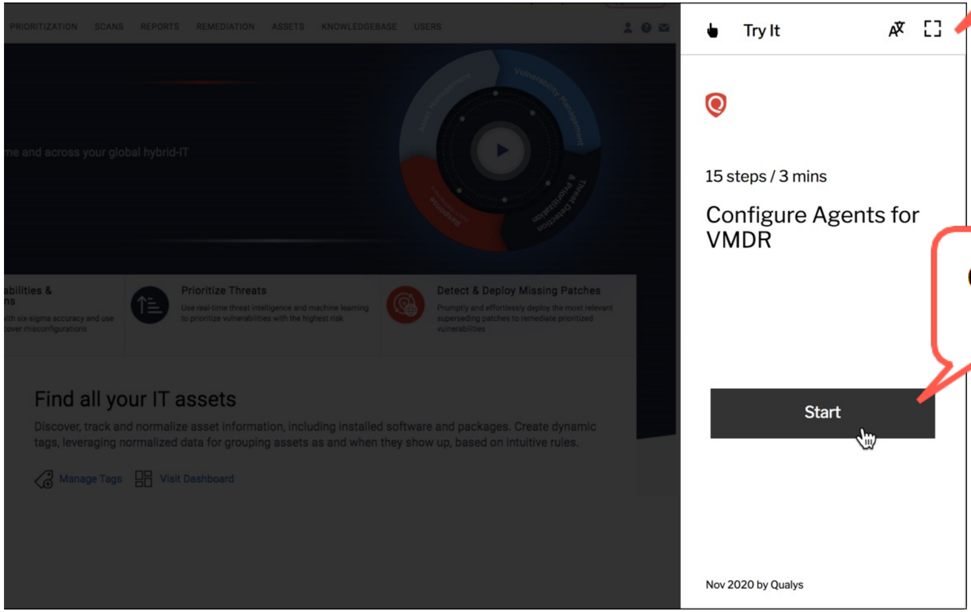


Navigate to the following URL to view the “Configure Agents for VMDR” tutoria

PLAY http://ior.ad/7bZE

Click to open Lab Tutorial. 1

Maximize Screen 2



me and across your global hybrid-IT

abilities & ns

Prioritize Threats

Detect & Deploy Missing Patches

Find all your IT assets

Discover, track and normalize asset information, including installed software and packages. Create dynamic tags, leveraging normalized data for grouping assets as and when they show up, based on intuitive rules.

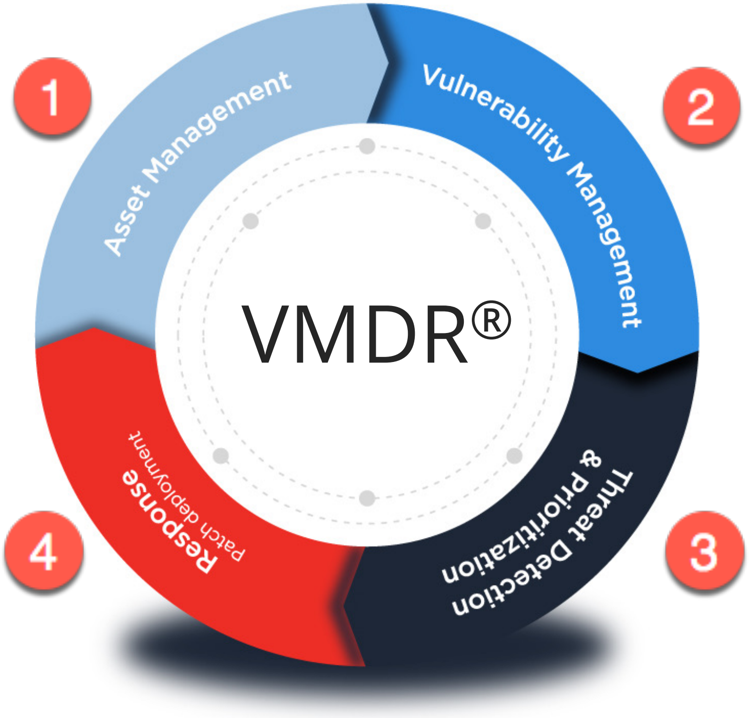
15 steps / 3 mins

Configure Agents for VMDR

Nov 2020 by Qualys

Click Start Button 3

Qualys VMDR Lifecycle



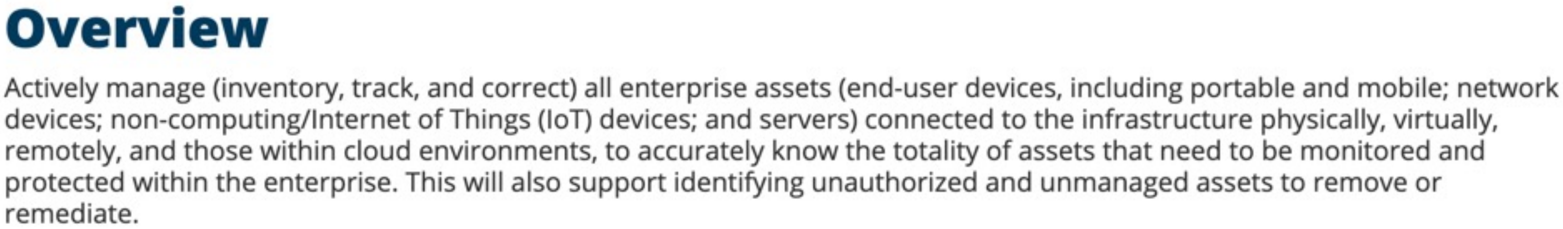
Qualys.

VMDR Agenda

1. Asset Management
   - Qualys Sensor Overview
   - CyberSecurity Asset Management (CSAM)
2. Vulnerability Management (VM)
   - Vulnerability Findings
   - Dashboards & Widgets
3. Threat Detection & Prioritization (TP)
   - VMDR Threat Feed
   - VMDR Prioritization Report
4. Response – Patch Management (PM)
   - Deployment Jobs
   - Patch Catalog

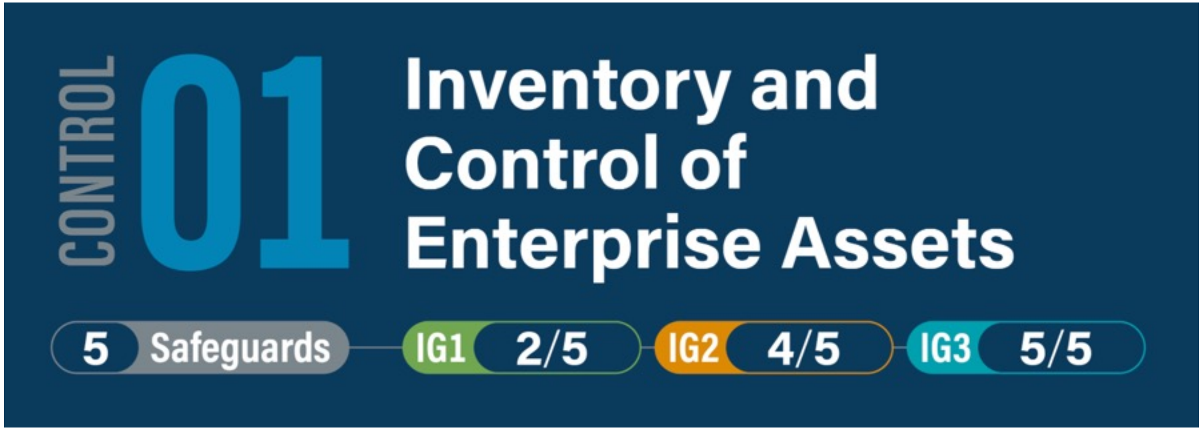
Asset Management

CIS Control 1: Inventory and Control of Enterprise Assets



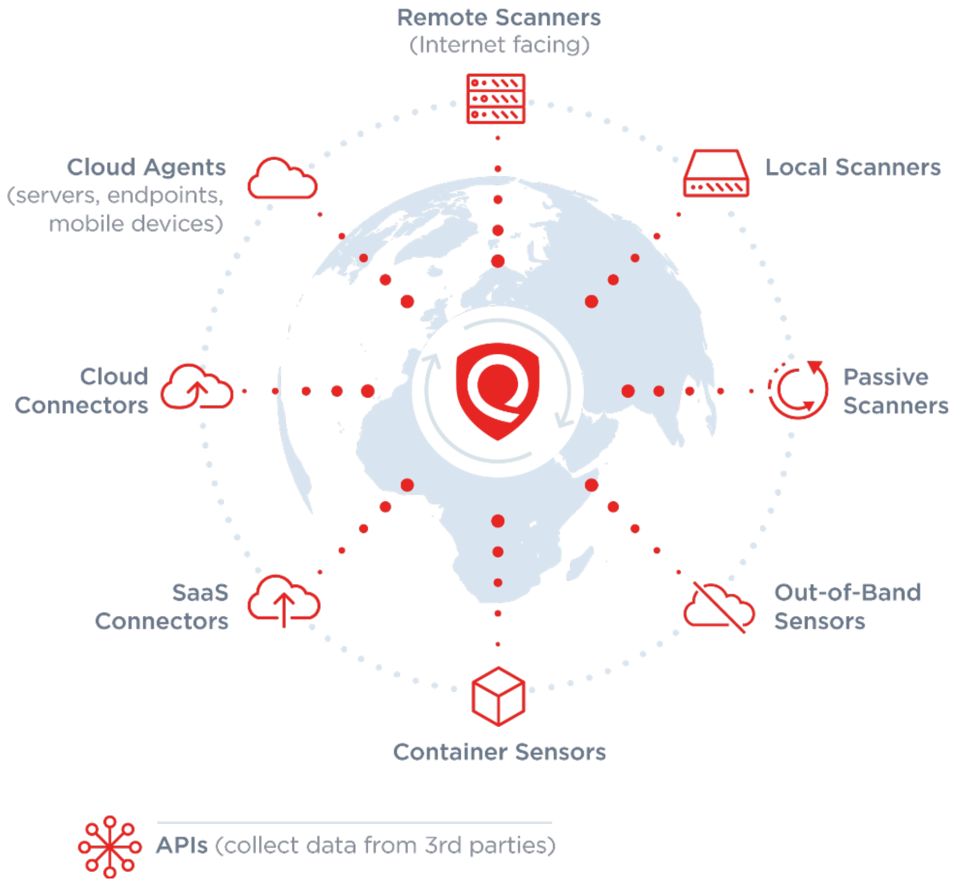
Overview

Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.



https://www.cisecurity.org/controls/inventory-and-control-of-enterprise-assets/

Qualys Sensor Platform



Remote Scanners
(Internet facing)

Local Scanners

Passive
Scanners

Out-of-Band
Sensors

Container Sensors

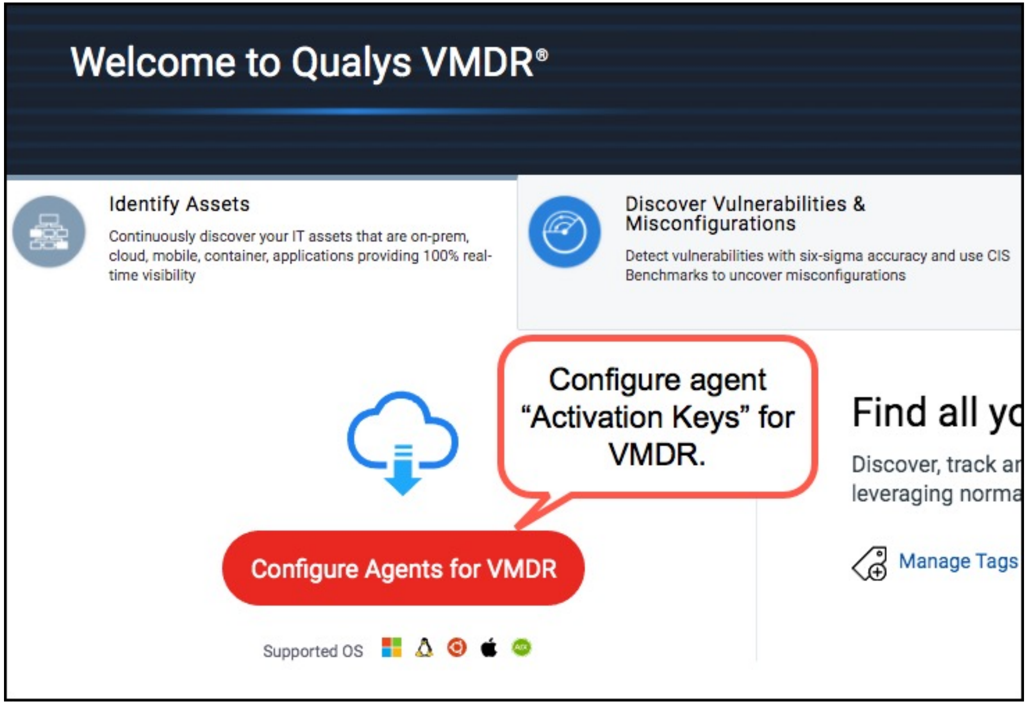
SaaS
Connectors

Cloud
Connectors

Cloud Agents
(servers, endpoints,
mobile devices)

APIs (collect data from 3rd parties)

Configure Agents for VMDR



Welcome to Qualys VMDR®

Identify Assets

Continuously discover your IT assets that are on-prem, cloud, mobile, container, applications providing 100% real-time visibility

Discover Vulnerabilities & Misconfigurations

Detect vulnerabilities with six-sigma accuracy and use CIS Benchmarks to uncover misconfigurations

Configure agent "Activation Keys" for VMDR.

Find all yo

Discover, track ar leveraging norma

- The patching and response functions in VMDR require Cloud Agent.
- Some Agent Activation Keys may need to be updated to include the VMDR application modules (i.e., VM, CSAM, SCA, and PM).

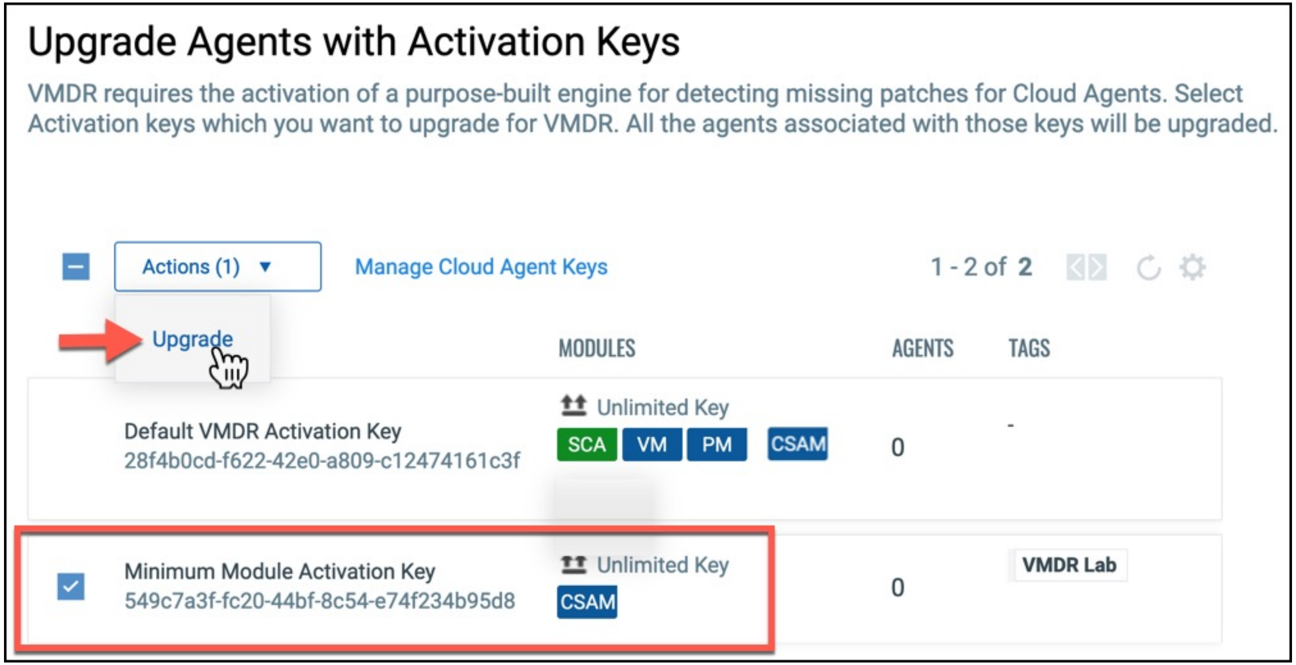
Lab 1: Configure Agents for VMDR

Please consult pages 3 to 14 in the lab tutorial supplement for details.

PLAY Tutorial begins on page 4.

10 mins

Upgrade Agent Activation Keys



Upgrade Agents with Activation Keys

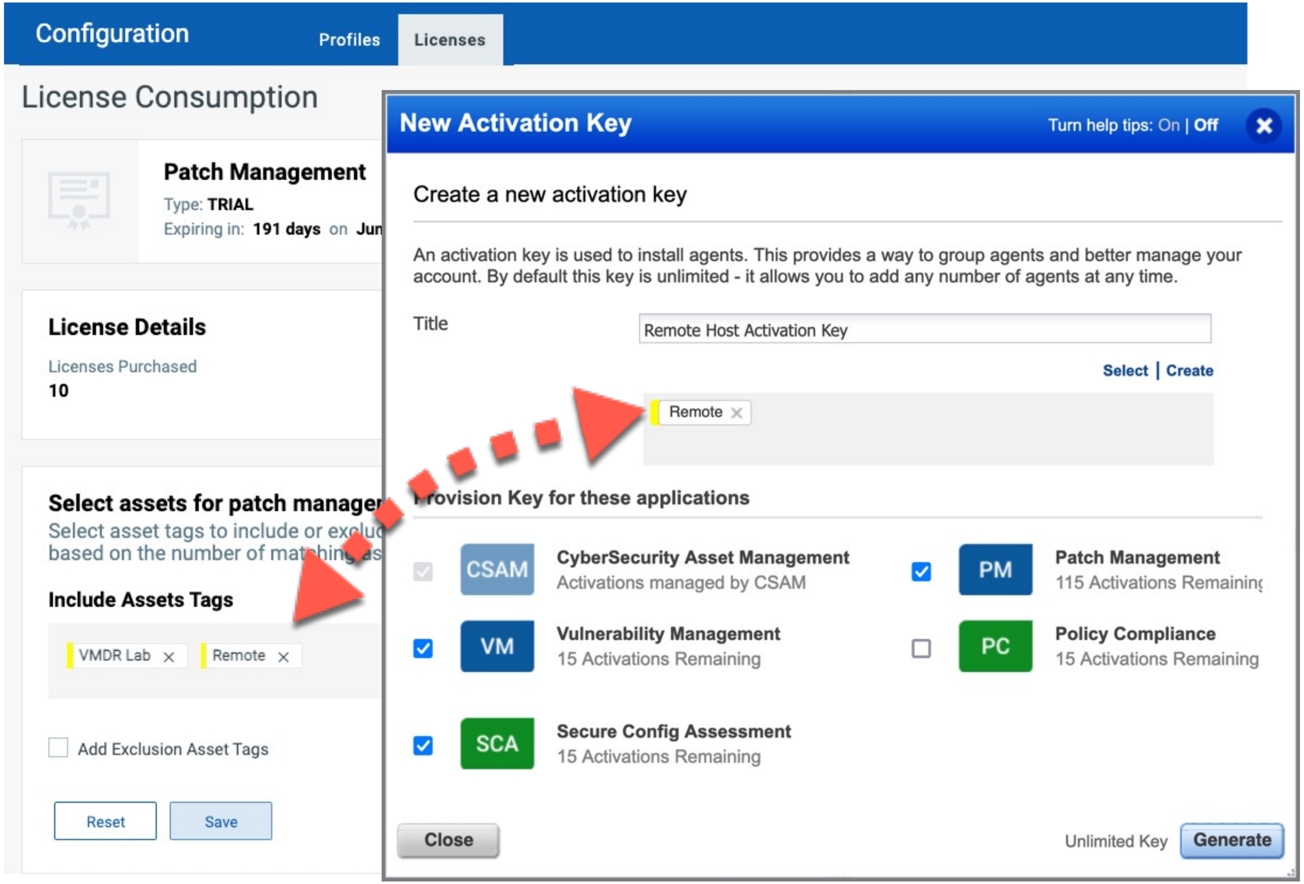
VMDR requires the activation of a purpose-built engine for detecting missing patches for Cloud Agents. Select Activation keys which you want to upgrade for VMDR. All the agents associated with those keys will be upgraded.

		MODULES	AGENTS	TAGS
	Default VMDR Activation Key 28f4b0cd-f622-42e0-a809-c12474161c3f	Unlimited Key SCA VM PM CSAM	0	-
☑	Minimum Module Activation Key 549c7a3f-fc20-44bf-8c54-e74f234b95d8	Unlimited Key CSAM	0	VMDR Lab

Upgrade Agent Activation Keys to include VMDR application modules (i.e., VM, SCA, PM, CSAM).

Activation Key Tagging Strategy

BEST PRACTICE: Assign "static" tags to agent Activation Keys and use them to ensure agent hosts receive their appropriate performance settings, patching licenses, and patch job assignments.



Configuration | Profiles | Licenses

License Consumption

Patch Management
Type: TRIAL
Expiring in: 191 days on Jun

License Details
Licenses Purchased
10

Select assets for patch manager
Select asset tags to include or exclud
based on the number of matching as

Include Assets Tags
VMDR Lab × Remote ×

☐ Add Exclusion Asset Tags

Reset | Save

New Activation Key — Turn help tips: On | Off

Create a new activation key

An activation key is used to install agents. This provides a way to group agents and better manage your account. By default this key is unlimited - it allows you to add any number of agents at any time.

Title: Remote Host Activation Key

Select | Create

Remote ×

Provision Key for these applications

- ☑ CSAM — **CyberSecurity Asset Management** — Activations managed by CSAM
- ☑ PM — **Patch Management** — 115 Activations Remaining
- ☑ VM — **Vulnerability Management** — 15 Activations Remaining
- ☐ PC — **Policy Compliance** — 15 Activations Remaining
- ☑ SCA — **Secure Config Assessment** — 15 Activations Remaining

Close | Unlimited Key | Generate

Qualys.

CyberSecurity Asset Management

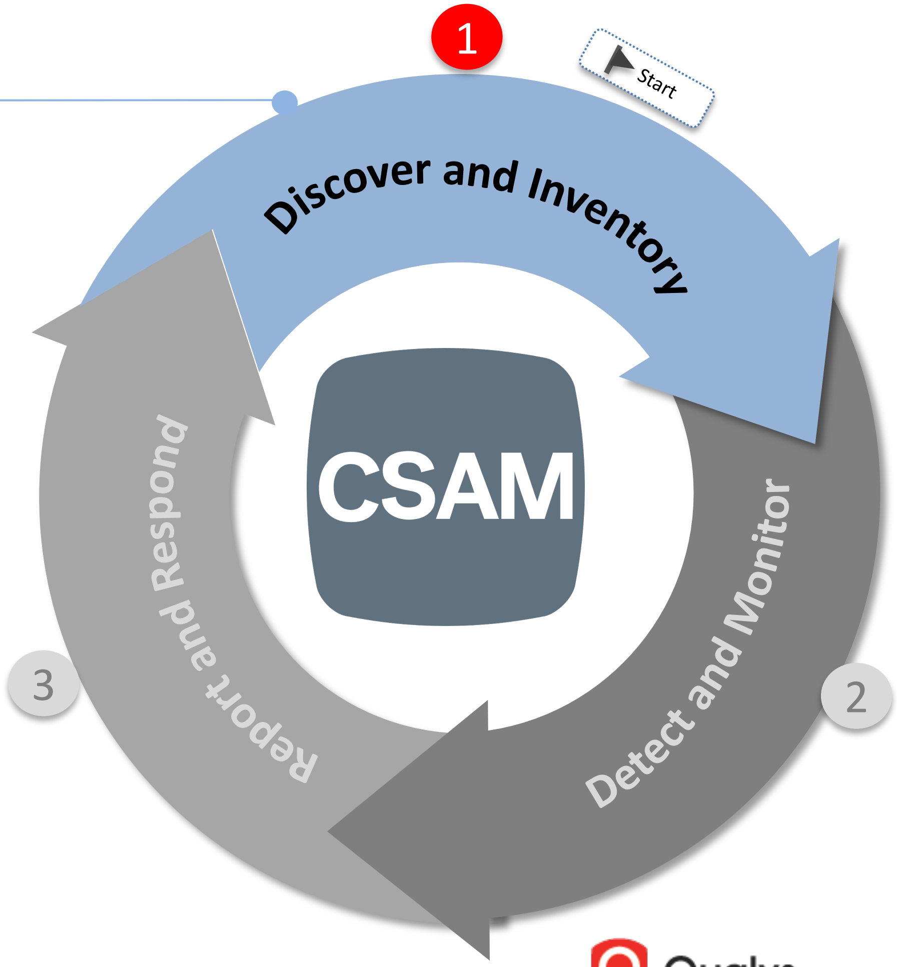
Discover and Inventory Assets

Asset Inventory Data Collection

- Passive Sensor
- Configure CMDB Sync (if using CMDB solution)

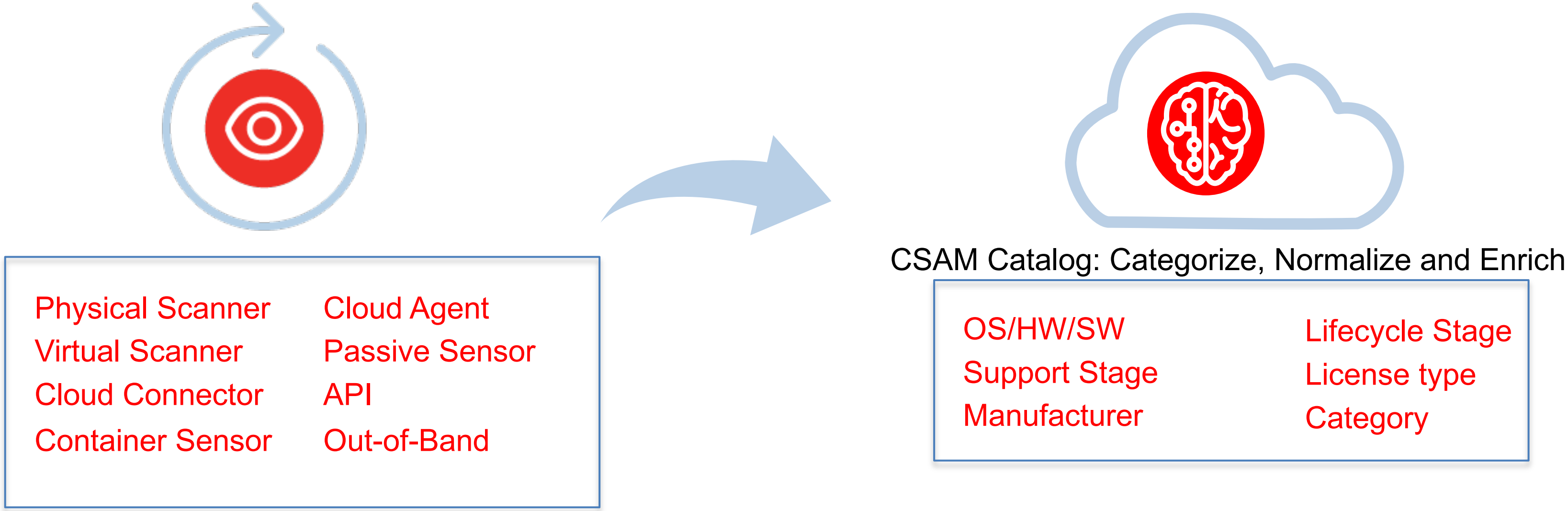
Normalization, Categorization & Enrichment* (performed automatically in the Qualys Cloud Platform)

Organize and Manage Assets (configure Asset Tags)



Qualys.

Comprehensive Asset & Software Inventory



Physical Scanner
Virtual Scanner
Cloud Connector
Container Sensor

Cloud Agent
Passive Sensor
API
Out-of-Band

CSAM Catalog: Categorize, Normalize and Enrich

OS/HW/SW
Support Stage
Manufacturer

Lifecycle Stage
License type
Category

Qualys CyberSecurity Asset Management (CSAM) aggregates data from all sensors.

Qualys Categorization, Normalization & Enrichment

	Operating Systems	Hardware	Software
Raw Data	Base OS Runtime AIX: 06.01.0009.0300 EE	Dell, Inc. R510	mysql-community-server 5.6.35-2.el7.x86_64
Category	UNIX > Server	Computers > Server	Databases > RDBMS
Manufacturer	IBM	Dell	Sun Microsystems
Owner	IBM	Dell	Oracle
Product	AIX	PowerEdge	MySQL Server
Market Version / Model	6	R510	5
Edition	Enterprise	-	Community
Version	6.1	-	5.6
Update	TL9 SP3	-	35-2.el6
Architecture	64-Bit	-	64-Bit
Lifecycle Stage	EOL/EOS	OBS	EOL
End-of-Life	30-Apr-2015	1-Sep-2012	28-Feb-2018
End-of-Support	30-Apr-2017	1-Sep-2012	28-Feb-2021
Support Stage	Unsupported	Obsolete	Extended Support
License Type	Commercial	-	Open Source (GPL-2.0)

Normalization & categorization

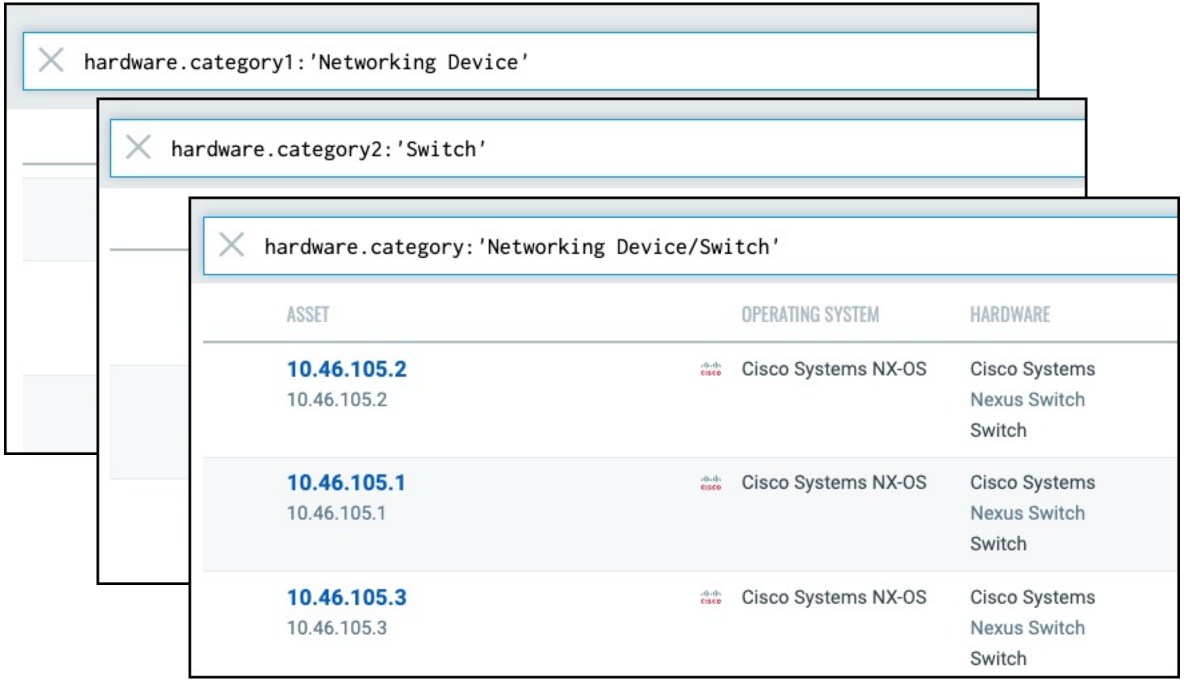
Advanced asset information

Search Hardware Categories

hardware.category1: value1
hardware.category2: value2
hardware.category: value1 / value2

→

hardware.category1: `Networking Device`
hardware.category2: `Switch`
hardware.category: `Networking Device / Switch`



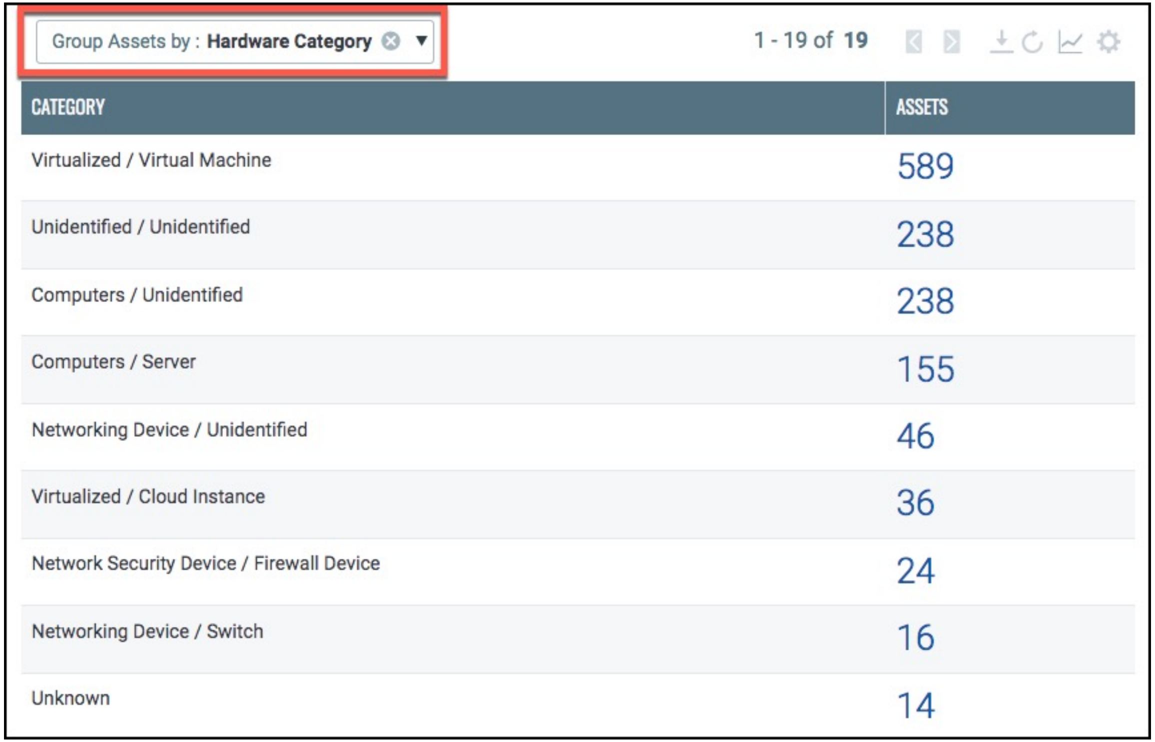
```
hardware.category1:'Networking Device'
```

```
hardware.category2:'Switch'
```

```
hardware.category:'Networking Device/Switch'
```

ASSET	OPERATING SYSTEM	HARDWARE
10.46.105.2 10.46.105.2	Cisco Systems NX-OS	Cisco Systems Nexus Switch Switch
10.46.105.1 10.46.105.1	Cisco Systems NX-OS	Cisco Systems Nexus Switch Switch
10.46.105.3 10.46.105.3	Cisco Systems NX-OS	Cisco Systems Nexus Switch Switch

Hardware Category List



Group Assets by : **Hardware Category** ▾

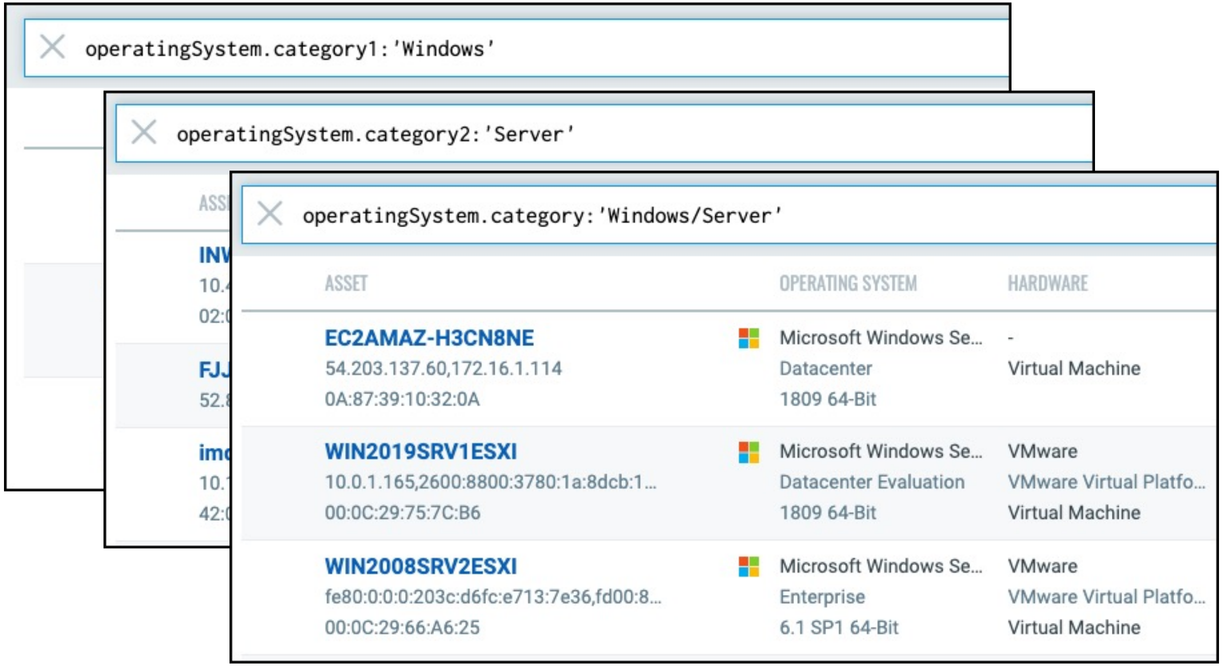
1 - 19 of **19**

CATEGORY	ASSETS
Virtualized / Virtual Machine	589
Unidentified / Unidentified	238
Computers / Unidentified	238
Computers / Server	155
Networking Device / Unidentified	46
Virtualized / Cloud Instance	36
Network Security Device / Firewall Device	24
Networking Device / Switch	16
Unknown	14

Group assets by Hardware Category to build a list of hardware category values in your account.

Search OS Categories

```
operatingSystem.category1: value1                  operatingSystem.category1: `Windows`
operatingSystem.category2: value2          →       operatingSystem.category2: `Server`
operatingSystem.category: value1 / value2          operatingSystem.category: `Windows / Server`
```



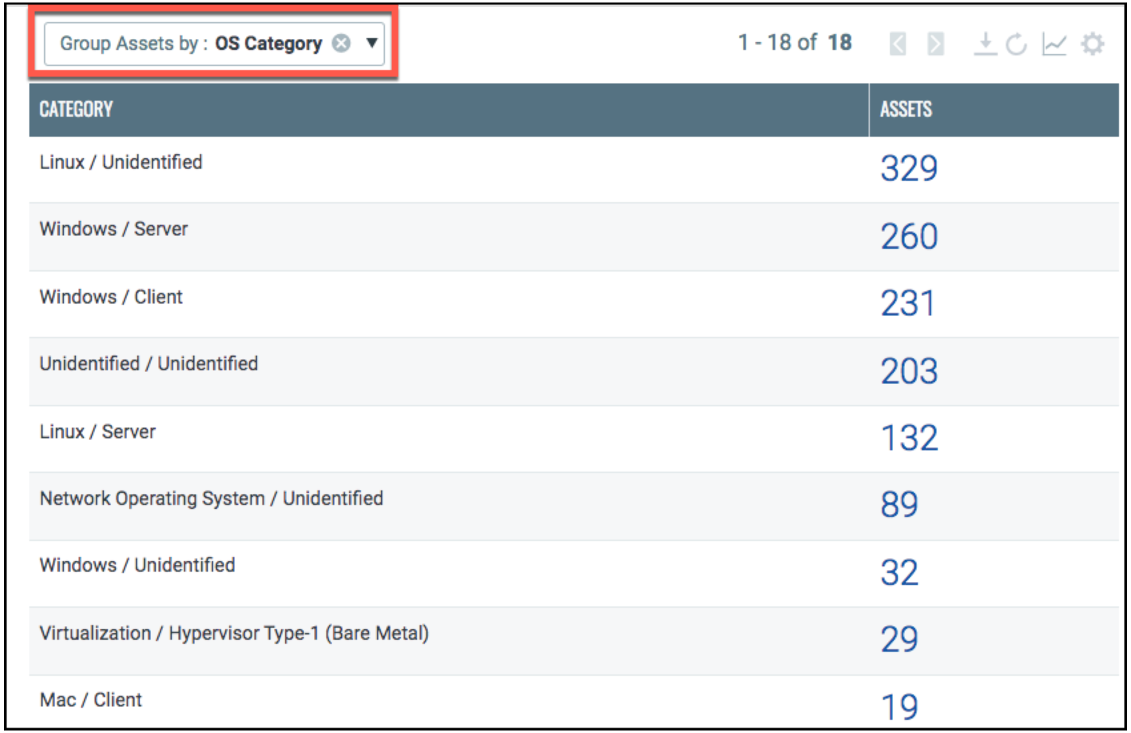
```
operatingSystem.category1:'Windows'
```

```
operatingSystem.category2:'Server'
```

```
operatingSystem.category:'Windows/Server'
```

ASSET	OPERATING SYSTEM	HARDWARE
EC2AMAZ-H3CN8NE 54.203.137.60,172.16.1.114 0A:87:39:10:32:0A	Microsoft Windows Se... Datacenter 1809 64-Bit	- Virtual Machine
WIN2019SRV1ESXI 10.0.1.165,2600:8800:3780:1a:8dcb:1... 00:0C:29:75:7C:B6	Microsoft Windows Se... Datacenter Evaluation 1809 64-Bit	VMware VMware Virtual Platfo... Virtual Machine
WIN2008SRV2ESXI fe80:0:0:0:203c:d6fc:e713:7e36,fd00:8... 00:0C:29:66:A6:25	Microsoft Windows Se... Enterprise 6.1 SP1 64-Bit	VMware VMware Virtual Platfo... Virtual Machine

OS Category List



CATEGORY	ASSETS
Linux / Unidentified	329
Windows / Server	260
Windows / Client	231
Unidentified / Unidentified	203
Linux / Server	132
Network Operating System / Unidentified	89
Windows / Unidentified	32
Virtualization / Hypervisor Type-1 (Bare Metal)	29
Mac / Client	19

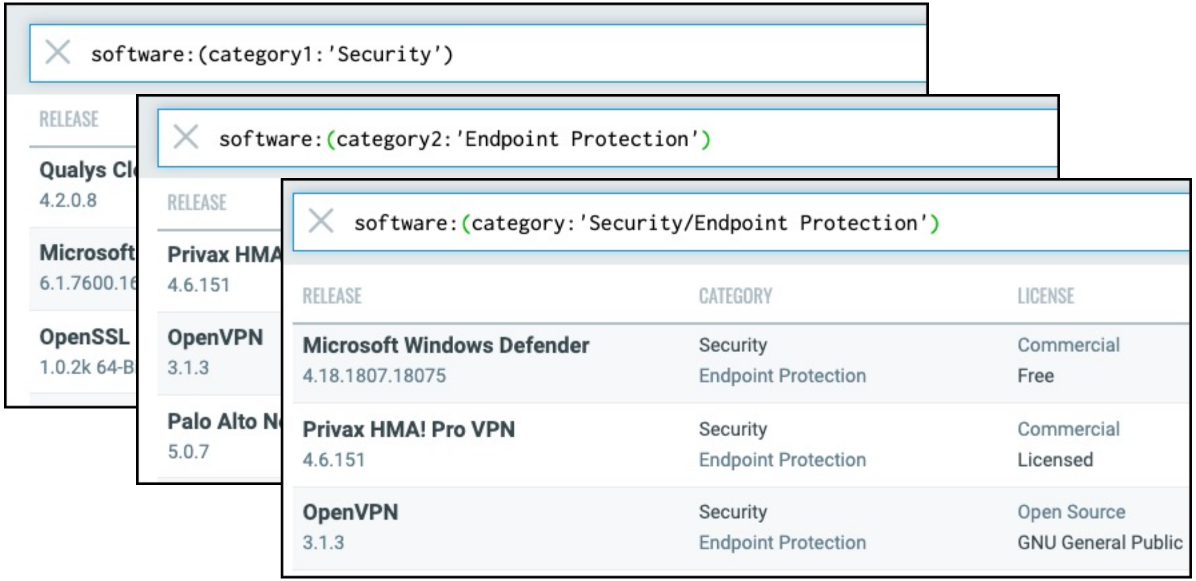
Group assets by OS Category to build a list of operating system category values in your account.

Search Software Categories

software:(category1: value1)
software:(category2: value2)
software:(category: value1 / value2)

→

software:(category1: `Security`)
software:(category2: `Endpoint Protection`)
software:(category: `Security / Endpoint Protection`)



```
software:(category1:'Security')
```

RELEASE

Qualys Cl
4.2.0.8

Microsoft
6.1.7600.16

OpenSSL
1.0.2k 64-B

```
software:(category2:'Endpoint Protection')
```

RELEASE

Privax HMA
4.6.151

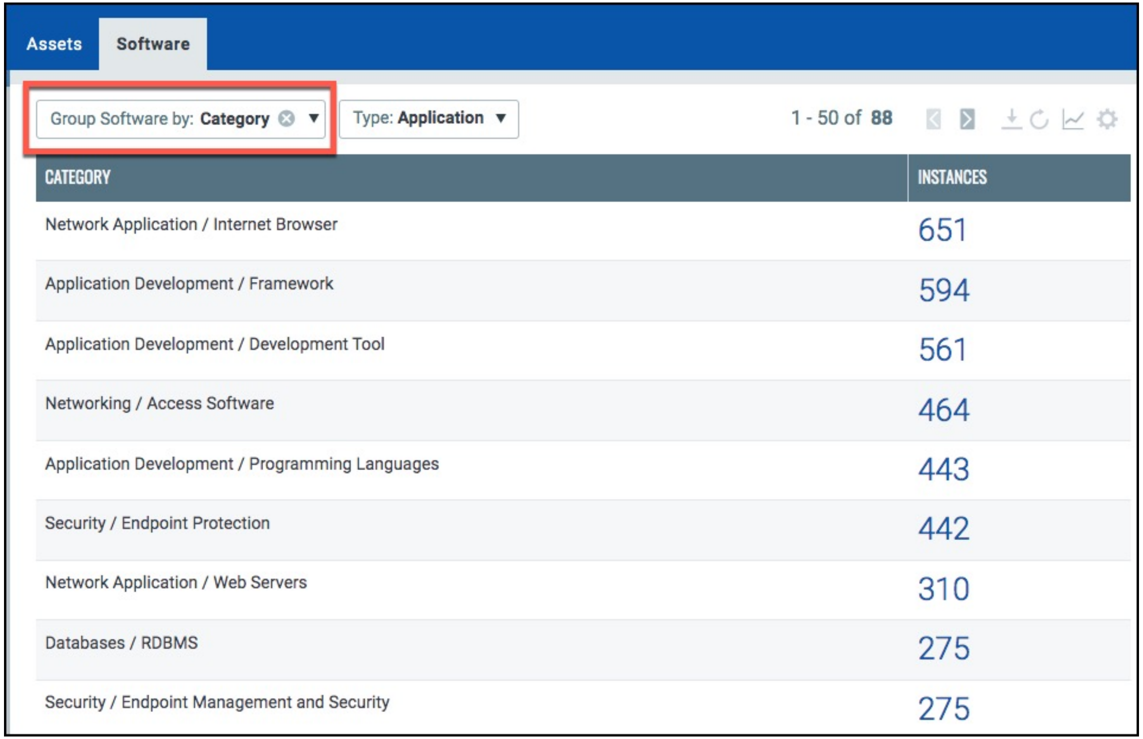
OpenVPN
3.1.3

Palo Alto N
5.0.7

```
software:(category:'Security/Endpoint Protection')
```

RELEASE	CATEGORY	LICENSE
Microsoft Windows Defender 4.18.1807.18075	Security Endpoint Protection	Commercial Free
Privax HMA! Pro VPN 4.6.151	Security Endpoint Protection	Commercial Licensed
OpenVPN 3.1.3	Security Endpoint Protection	Open Source GNU General Public

Software Category List



Group Software by: **Category** ▾   Type: **Application** ▾   1 - 50 of **88**

CATEGORY	INSTANCES
Network Application / Internet Browser	651
Application Development / Framework	594
Application Development / Development Tool	561
Networking / Access Software	464
Application Development / Programming Languages	443
Security / Endpoint Protection	442
Network Application / Web Servers	310
Databases / RDBMS	275
Security / Endpoint Management and Security	275

Group Software by Category to build a list of software category values in your account.

Lab 2 : Search Using Categories

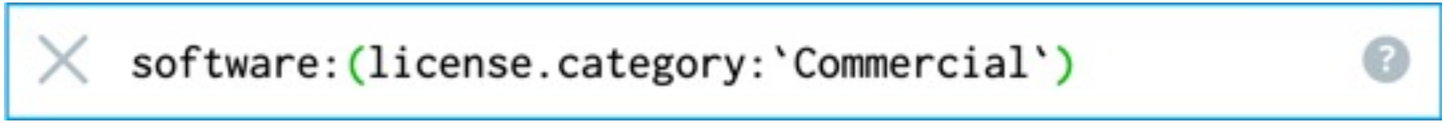
Please consult pages 15 to 16 in the lab tutorial supplement for details.

PLAY Tutorial begins on page 16.

5 mins

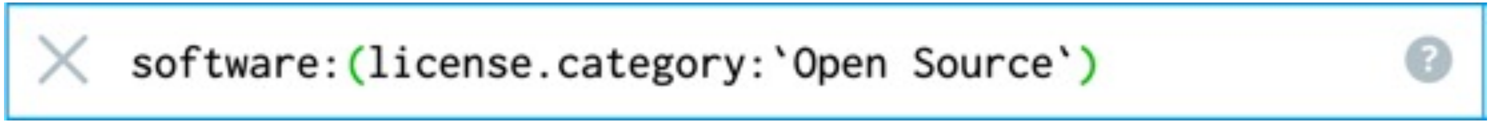
Software License Category

Commercial – Supported by vendor.



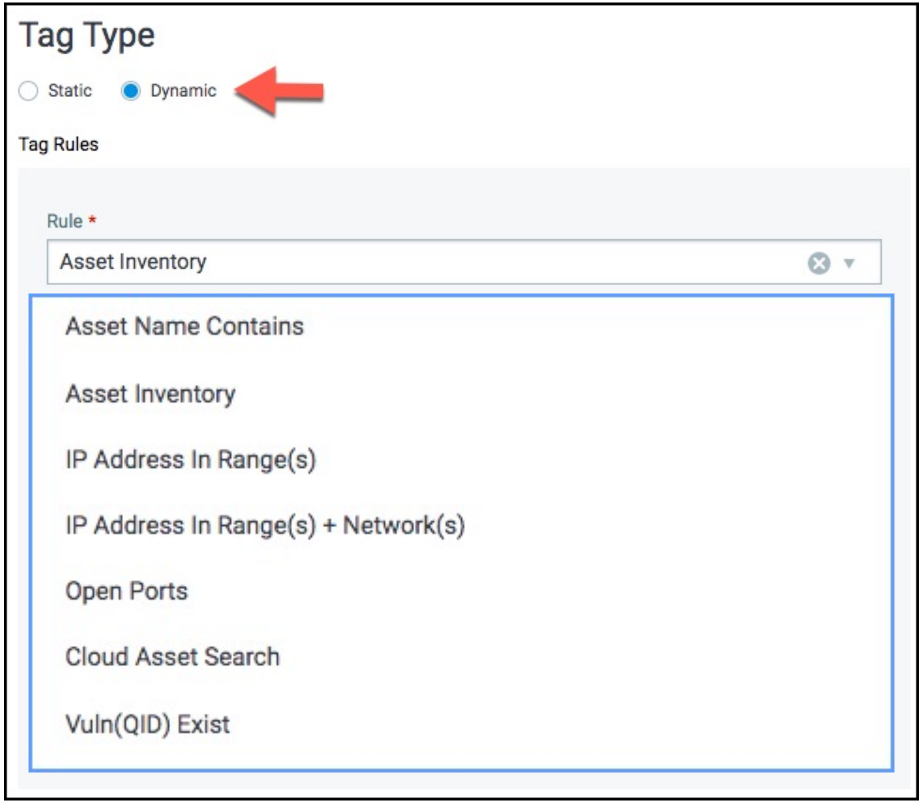
```
software:(license.category:`Commercial`)
```

Open Source – Free for public use.



```
software:(license.category:`Open Source`)
```

Dynamic Rule-Based Tags



Tag Type

○ Static ● Dynamic

Tag Rules

Rule *

Asset Inventory

- The “Asset Inventory” rule engine allows you to build tags using query tokens, including the Hardware, OS, and Software category tokens.
- Other “dynamic” rule engines are also available.

Lab 3 : Dynamic Rule-Based Tags

Please consult pages 17 in the lab tutorial supplement for details.

PLAY Tutorial begins on page 17.

5 mins

Unidentified vs. Unknown

Some OS and Hardware assets may appear as “unidentified” or “unknown.”

Unidentified

- Not enough data has been discovered/collected for Qualys to determine the asset’s hardware or operating system.

Unknown

- Adequate data exists for Qualys to categorize the asset, but it has yet to be cataloged.

Network Passive Sensor

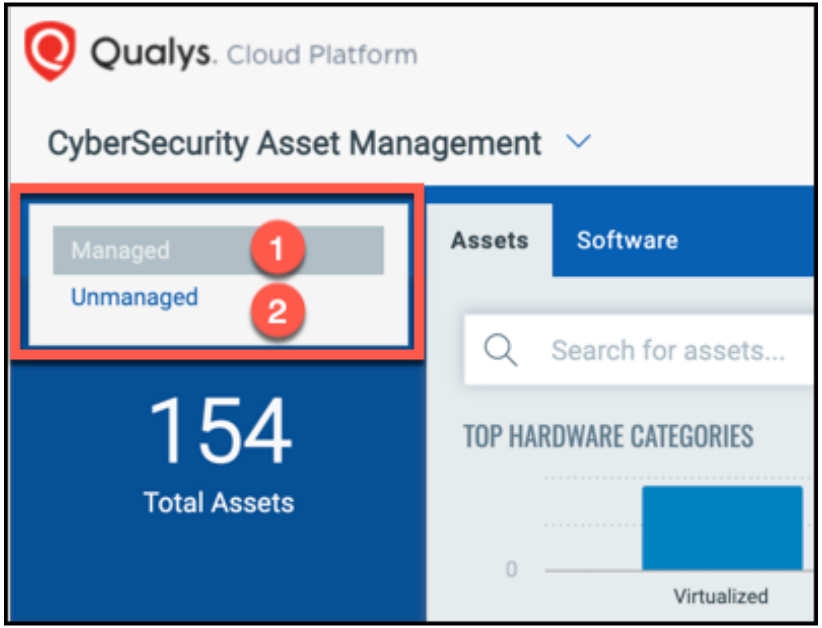
Passive Sensor Overview

- Sniffs traffic via network TAP or the SPAN port of a network switch.
- Captured data and traffic is sent to the Qualys Platform for analysis and processing.

1. Discovered assets not in your account, are placed in the “Unmanaged” section of Qualys CSAM.
2. Enable “Traffic Analysis” to reveal communication between assets, including conversations between managed and unmanaged assets.

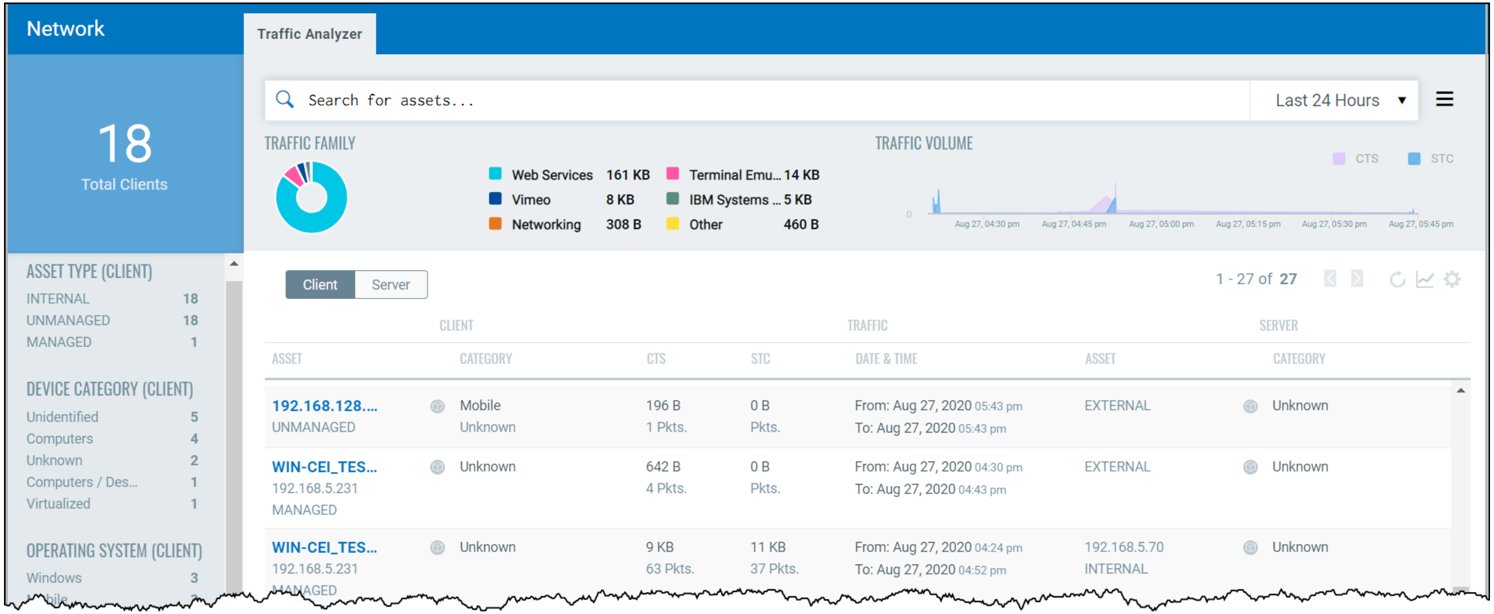
Managed vs. Unmanaged Assets

1. If discovered data is confirmed to match an asset already in your account, its information can be merged with the existing asset.
2. Discovered assets not in your account, are placed in the “Unmanaged” section of Qualys CSAM.



Network Traffic Analyzer

- Conversations between assets can offer new discoveries and insights.



18
Total Clients

ASSET TYPE (CLIENT)

INTERNAL	18
UNMANAGED	18
MANAGED	1

DEVICE CATEGORY (CLIENT)

Unidentified	5
Computers	4
Unknown	2
Computers / Des...	1
Virtualized	1

OPERATING SYSTEM (CLIENT)

Windows	3
Mobile	2

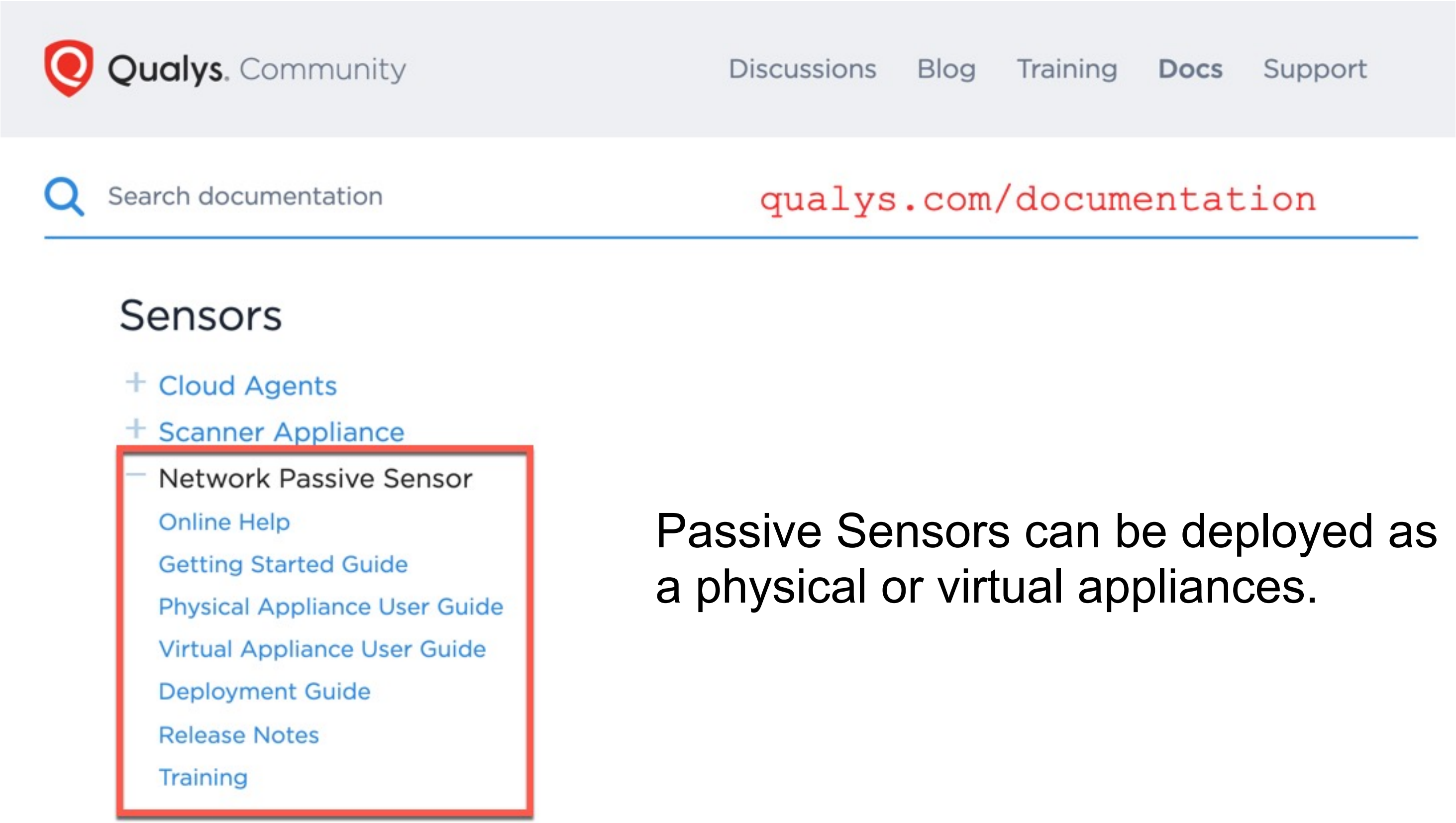
TRAFFIC FAMILY

Web Services	161 KB	Terminal Emu...	14 KB
Vimeo	8 KB	IBM Systems ...	5 KB
Networking	308 B	Other	460 B

TRAFFIC VOLUME

CLIENT		TRAFFIC			SERVER	
ASSET	CATEGORY	CTS	STC	DATE & TIME	ASSET	CATEGORY
192.168.128.... UNMANAGED	Mobile Unknown	196 B 1 Pkts.	0 B Pkts.	From: Aug 27, 2020 05:43 pm To: Aug 27, 2020 05:43 pm	EXTERNAL	Unknown
WIN-CEI_TES... 192.168.5.231 MANAGED	Unknown	642 B 4 Pkts.	0 B Pkts.	From: Aug 27, 2020 04:30 pm To: Aug 27, 2020 04:43 pm	EXTERNAL	Unknown
WIN-CEI_TES... 192.168.5.231 MANAGED	Unknown	9 KB 63 Pkts.	11 KB 37 Pkts.	From: Aug 27, 2020 04:24 pm To: Aug 27, 2020 04:52 pm	192.168.5.70 INTERNAL	Unknown

Network Passive Sensor User Guides



Qualys. Community

Discussions Blog Training **Docs** Support

Search documentation

qualys.com/documentation

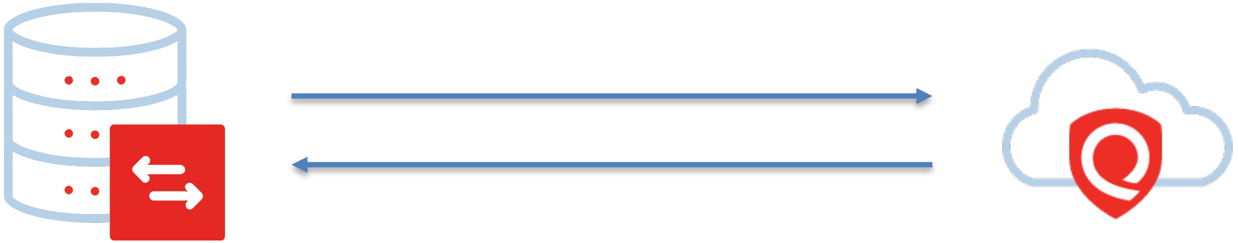
Sensors

- + Cloud Agents
- + Scanner Appliance
- − Network Passive Sensor
  - Online Help
  - Getting Started Guide
  - Physical Appliance User Guide
  - Virtual Appliance User Guide
  - Deployment Guide
  - Release Notes
  - Training

Passive Sensors can be deployed as a physical or virtual appliances.

CMDB Sync

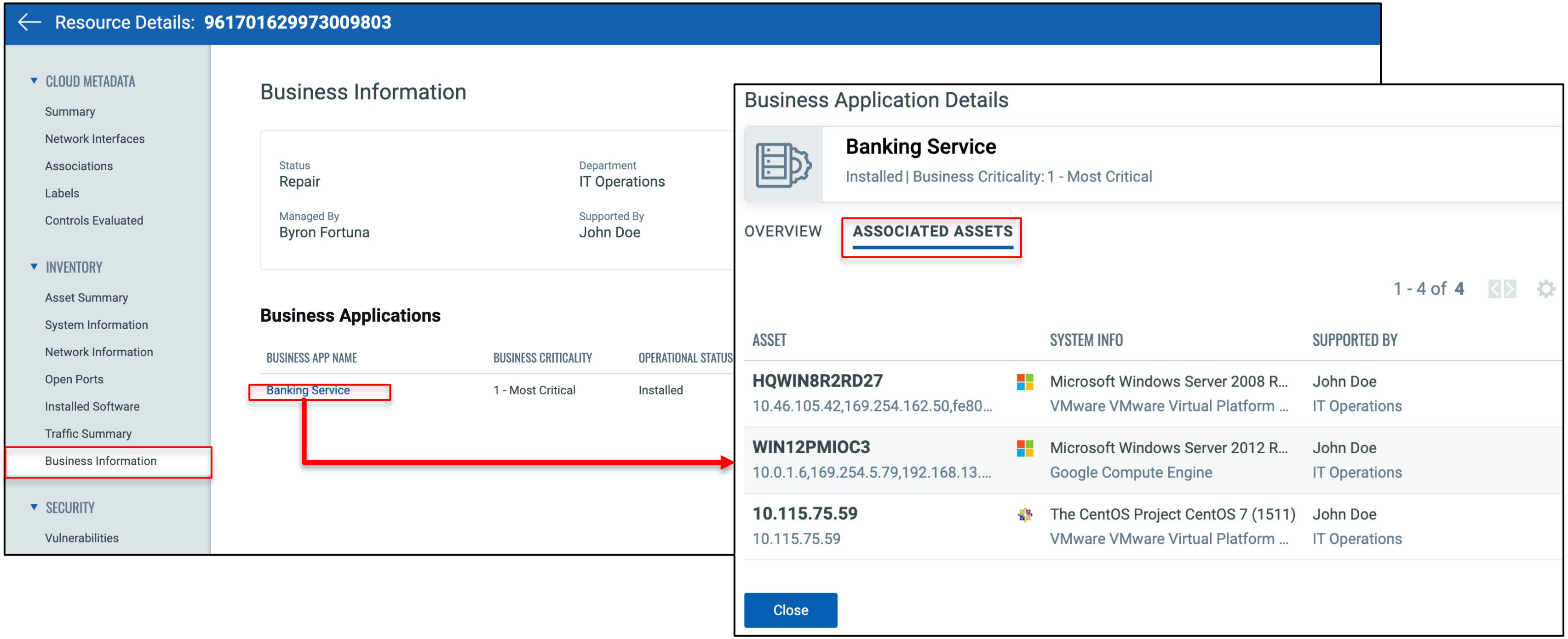
Certified ServiceNow CMDB Sync App



- Supports 2-way sync (Qualys to ServiceNow and ServiceNow to Qualys)
- Up-to-date, categorized, normalized, and enriched ServiceNow CMDB
- Enrich Qualys assets with key CMDB business data
- Synchronization schedules can be configured and saved.
- Asset metadata is only synchronized for assets that already exist in both Qualys and ServiceNow.
- Optionally, asset information is staged for user approval before being written to CMDB.

Qualys.

Import Business Attributes from ServiceNow CMDB



Business Information

Status
Repair

Department
IT Operations

Managed By
Byron Fortuna

Supported By
John Doe

Business Applications

BUSINESS APP NAME	BUSINESS CRITICALITY	OPERATIONAL STATUS
Banking Service	1 - Most Critical	Installed

Business Application Details

Banking Service
Installed | Business Criticality: 1 - Most Critical

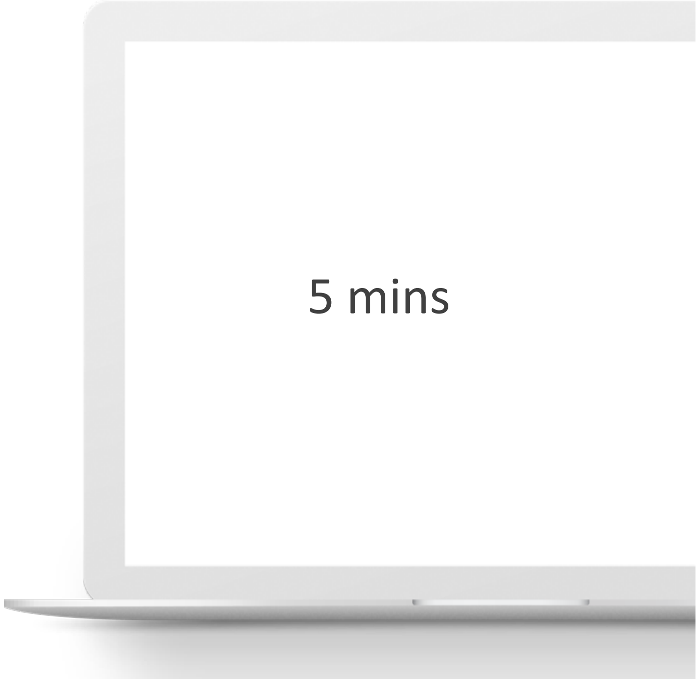
ASSET	SYSTEM INFO	SUPPORTED BY
HQWIN8R2RD27 10.46.105.42,169.254.162.50,fe80...	Microsoft Windows Server 2008 R... VMware VMware Virtual Platform ...	John Doe IT Operations
WIN12PMIOC3 10.0.1.6,169.254.5.79,192.168.13....	Microsoft Windows Server 2012 R... Google Compute Engine	John Doe IT Operations
10.115.75.59 10.115.75.59	The CentOS Project CentOS 7 (1511) VMware VMware Virtual Platform ...	John Doe IT Operations

- Automatically import business application and business context attributes from ServiceNow CMDB
- Identify other assets associated with a business application

Lab 4 : CMDB Sync and Business Context

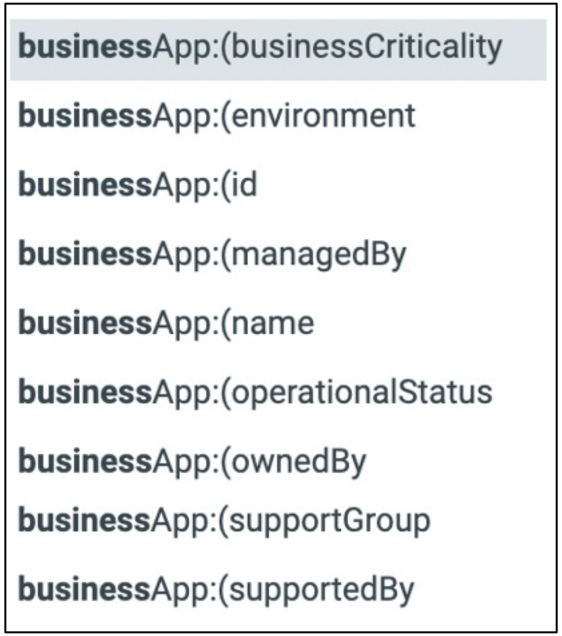
Please consult pages 19 to 20 in the lab tutorial supplement for details.

PLAY Tutorial begins on page 19.



5 mins

Use Business Attributes to Search for Assets



businessApp:(businessCriticality
businessApp:(environment
businessApp:(id
businessApp:(managedBy
businessApp:(name
businessApp:(operationalStatus
businessApp:(ownedBy
businessApp:(supportGroup
businessApp:(supportedBy

- Use any of the “businessApp” search tokens to single out assets, based on the business information and characteristics provided by ServiceNow.
- Queries using these tokens will impact assets already synchronized.

Integration with ServiceNow CMDB

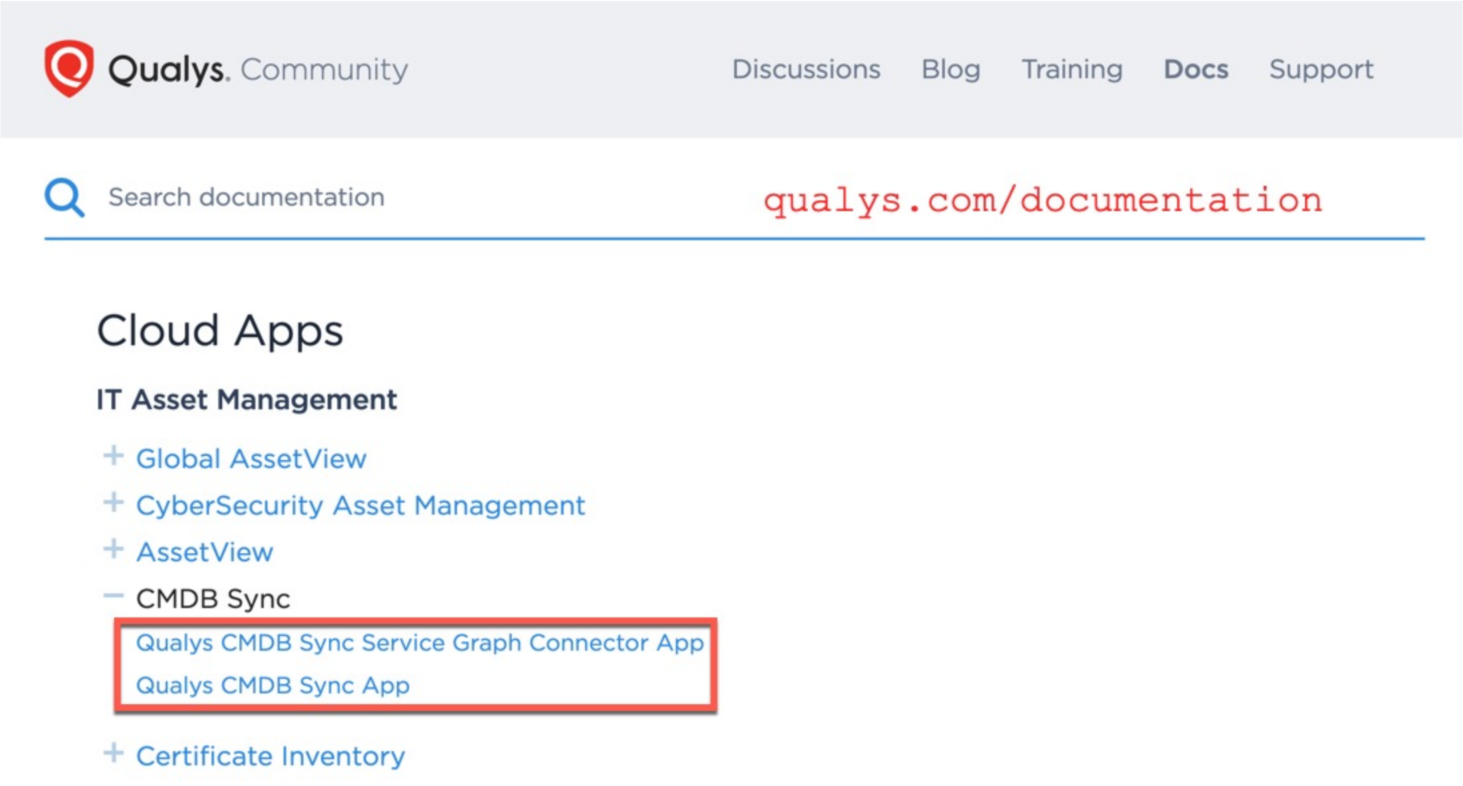
To implement ServiceNow CMDB Integration, a Qualys subscription with API access is required, along with the following application modules:

- CSAM
- Vulnerability Management

1. **Qualys CMDB Sync App**
   - Install the Qualys CMDB Sync App (available in ServiceNow Online Store)

2. **Qualys CMDB Sync Service Graph Connector App**
   - Install the Qualys Service Graph Connector App (available in ServiceNow Online Store)
   - ITOM Visibility license in ServiceNow

CMDB Sync App User Guides



Qualys. Community

Discussions Blog Training **Docs** Support

Search documentation

qualys.com/documentation

Cloud Apps

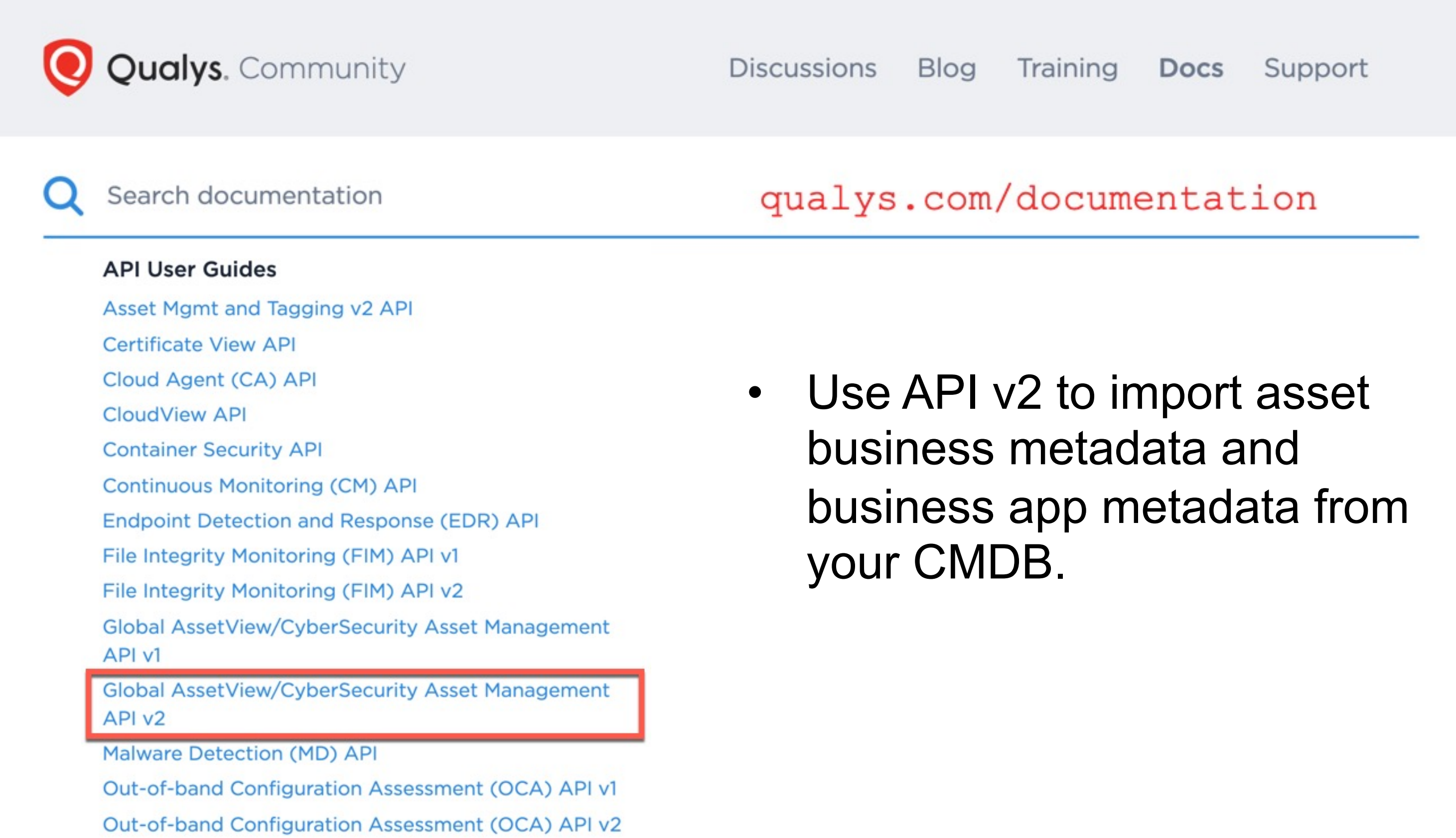
IT Asset Management

- + Global AssetView
- + CyberSecurity Asset Management
- + AssetView
- − CMDB Sync
  - Qualys CMDB Sync Service Graph Connector App
  - Qualys CMDB Sync App
- + Certificate Inventory

Public APIs for CMDB Sync

- CSAM now supports import of **Asset business metadata** and **Business app metadata** from your CMDB into your Qualys asset inventory (using v2 APIs).
- Imported business attributes are listed in the Asset Details page.
- User must have access to the CSAM module with API enabled for that role.
- Currently supports maximum 250 records for import in one API call for both Asset and Business app metadata.

API User Guide



Qualys. Community

Discussions Blog Training **Docs** Support

Search documentation

qualys.com/documentation

API User Guides

- Asset Mgmt and Tagging v2 API
- Certificate View API
- Cloud Agent (CA) API
- CloudView API
- Container Security API
- Continuous Monitoring (CM) API
- Endpoint Detection and Response (EDR) API
- File Integrity Monitoring (FIM) API v1
- File Integrity Monitoring (FIM) API v2
- Global AssetView/CyberSecurity Asset Management API v1
- Global AssetView/CyberSecurity Asset Management API v2
- Malware Detection (MD) API
- Out-of-band Configuration Assessment (OCA) API v1
- Out-of-band Configuration Assessment (OCA) API v2

- Use API v2 to import asset business metadata and business app metadata from your CMDB.

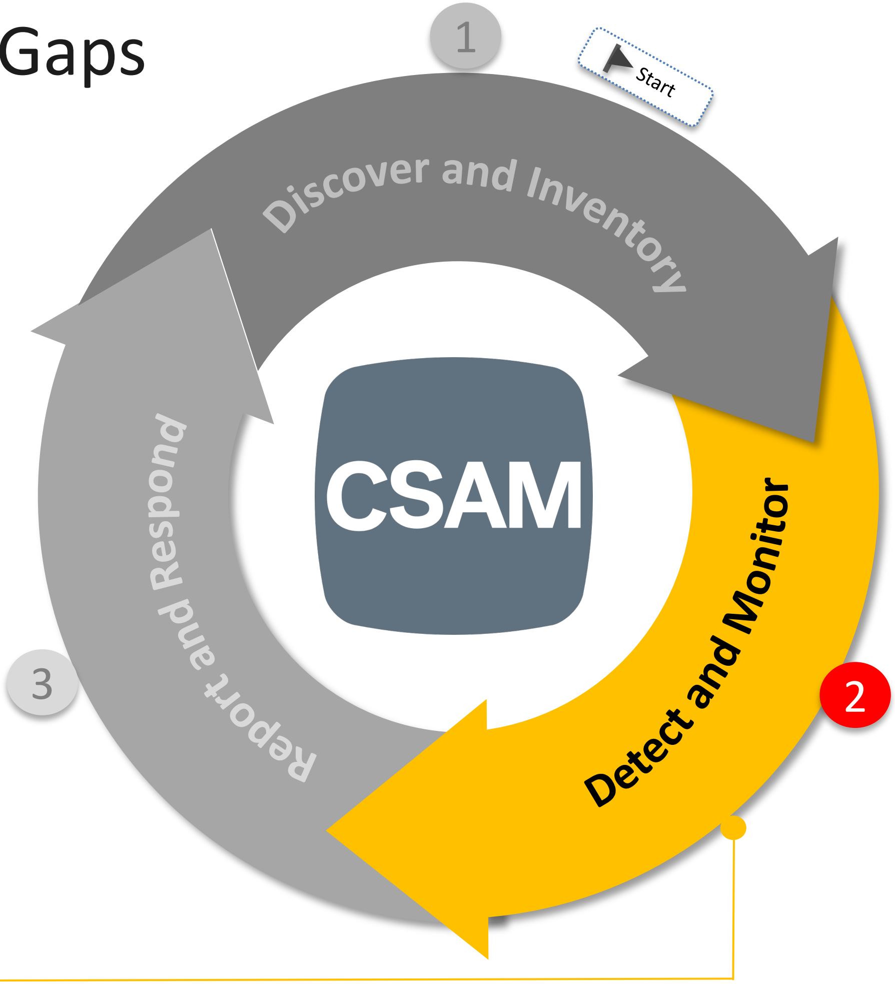
Detect and Monitor Security Gaps

Detect and Monitor Security Gaps

- **Asset Prioritization (**Define Asset Criticality Score)

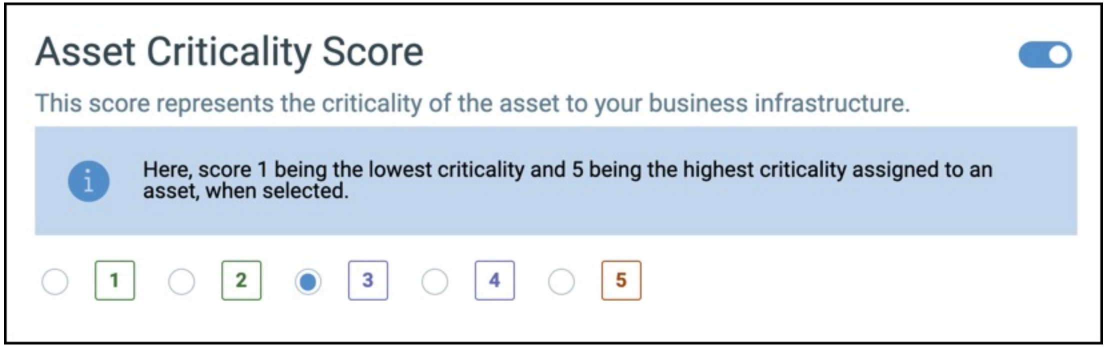
- **Product Lifecycle Management*** (EOL/EOS/Obsolete hardware and software automatically identified through enrichment in QCP)

- **Software Authorization*** (configure rules to identify authorized/unauthorized software)



Asset Criticality Score

Asset Criticality Score



Asset Criticality Score

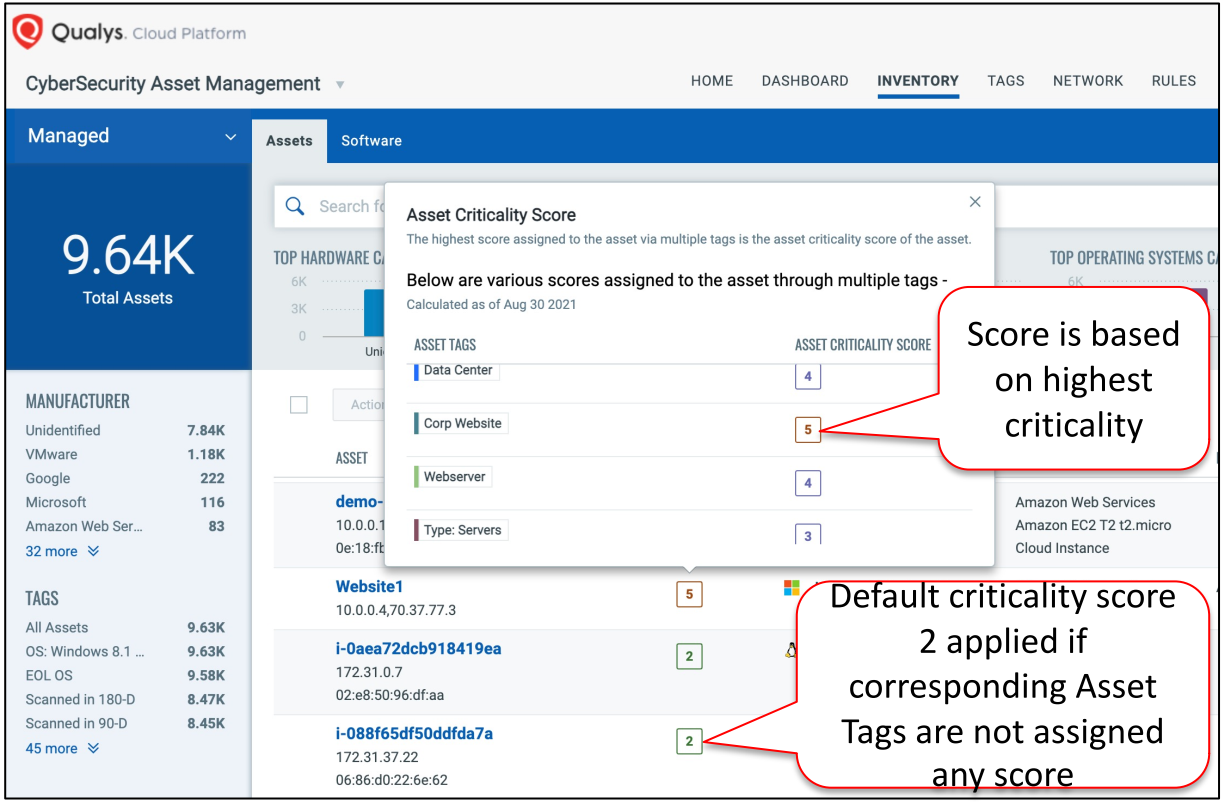
This score represents the criticality of the asset to your business infrastructure.

Here, score 1 being the lowest criticality and 5 being the highest criticality assigned to an asset, when selected.

○ 1 ○ 2 ● 3 ○ 4 ○ 5

- User defined scores
- Configured and implemented through Asset Tags
- Scale of 1 to 5:
  - 5 = most critical
  - 1= least critical

Asset Criticality Score



9.64K
Total Assets

MANUFACTURER

Unidentified	7.84K
VMware	1.18K
Google	222
Microsoft	116
Amazon Web Ser...	83

32 more

TAGS

All Assets	9.63K
OS: Windows 8.1 ...	9.63K
EOL OS	9.58K
Scanned in 180-D	8.47K
Scanned in 90-D	8.45K

45 more

Asset Criticality Score

The highest score assigned to the asset via multiple tags is the asset criticality score of the asset.

Below are various scores assigned to the asset through multiple tags -

Calculated as of Aug 30 2021

ASSET TAGS	ASSET CRITICALITY SCORE
Data Center	4
Corp Website	5
Webserver	4
Type: Servers	3

demo- 10.0.0.1 0e:18:fb		Amazon Web Services Amazon EC2 T2 t2.micro Cloud Instance
Website1 10.0.0.4,70.37.77.3	5	
i-0aea72dcb918419ea 172.31.0.7 02:e8:50:96:df:aa	2	
i-088f65df50ddfda7a 172.31.37.22 06:86:d0:22:6e:62	2	

Score is based on highest criticality

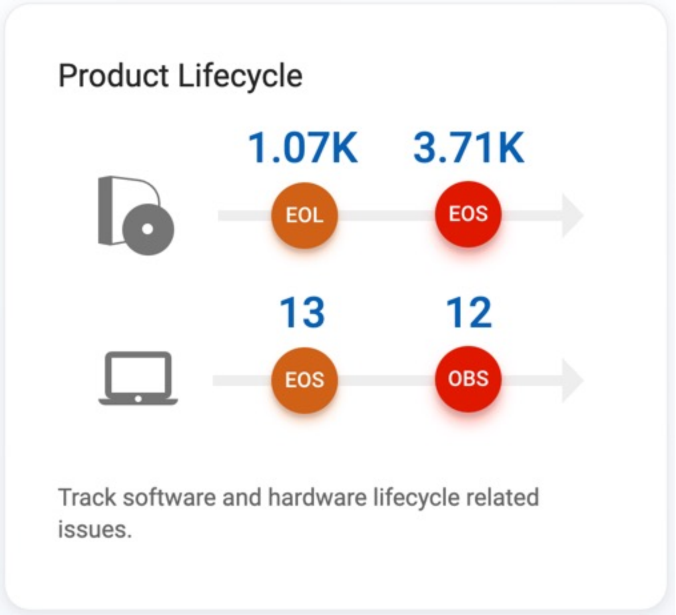
Default criticality score 2 applied if corresponding Asset Tags are not assigned any score

- An asset is scored by its tag with the highest criticality.
- Assets without scored tags will receive a default score of two (2).

Product Lifecycle Management

Product Lifecycle Information

- Identify EOL/EOS software and hardware
- Secure your environment by eliminating unsupported software and hardware
- Plan hardware refresh and software upgrades



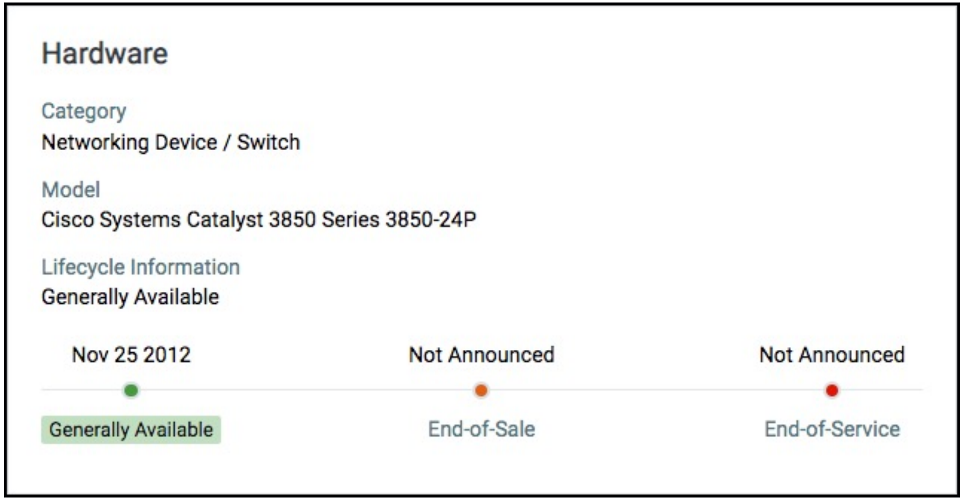
Product Lifecycle

Track software and hardware lifecycle related issues.

Hardware Lifecycle Stage

Search Token: `hardware.lifecycle.stage:`*`value`*

- **General Availability** (GA) - Hardware is in production, available for purchase, and supported
- **End of Sale** (EOS)- No longer being sold or by vendor
- **Obsolete** (OBS) - End-of-Service; no longer serviced via upgrades, patches, or maintenance



Hardware

Category
Networking Device / Switch

Model
Cisco Systems Catalyst 3850 Series 3850-24P

Lifecycle Information
Generally Available

Nov 25 2012	Not Announced	Not Announced
Generally Available	End-of-Sale	End-of-Service

Hardware Lifecycle Search Tokens

Attribute	Examples	Search Token
lifecycle stage	"INTRO", "GA", "EOS", "OBS"	hardware.lifecycle.stage
Introduction date	Feb-2015	hardware.lifecycle.intro
General Availability date	Apr-21-2014	hardware.lifecycle.ga
End-of-Sale date	May-2016	hardware.lifecycle.eos
Obsolete date	Jun-2018	hardware.lifecycle.obs

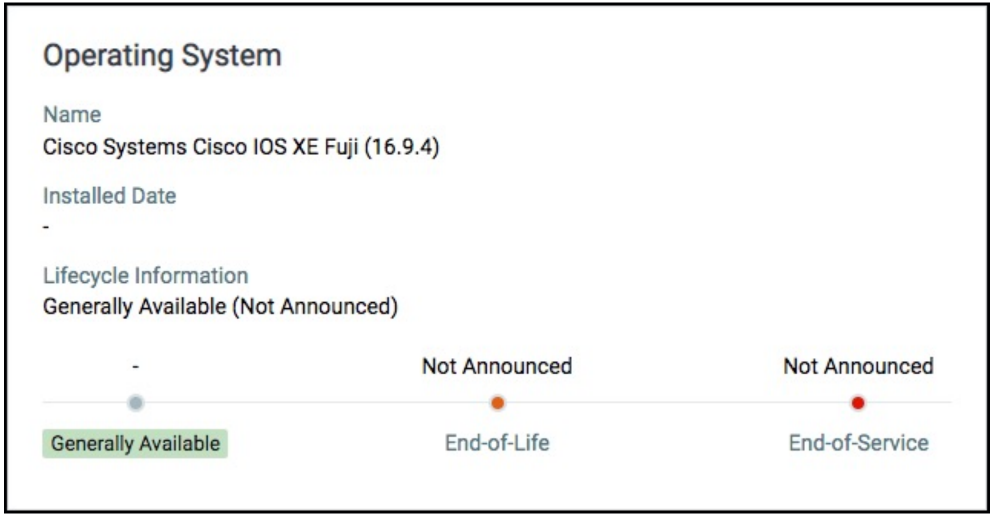
- The ‘lifecycle.stage’ token is useful when searching for the present stage of an asset.
- Use the other ‘lifecycle’ tokens to search for future EOS, and OBS dates.

OS & Software Lifecycle Stages

Search Tokens:

```
operatingSystem.lifecycle.stage:value
software:(lifecycle.stage:value)
```

- **Generally Available** (GA) - When the product became available for purchase.
- **End-of-Life** (EOL) - No longer marketing, selling, building new features, or promoting product (Security patches may still be provided).
- **End-of-Service** (EOS) - No longer serviced via upgrades, patches, or maintenance.



Operating System

Name

Cisco Systems Cisco IOS XE Fuji (16.9.4)

Installed Date

-

Lifecycle Information

Generally Available (Not Announced)

OS Lifecycle Search Tokens

Attribute	Examples	Search Token
Lifecycle state	"GA", "EOL", "EOS"	operatingSystem.lifecycle.stage
Support Stage	"Premier", "Extended", "Obsolete"	
General Availability date	Feb-15-2008	operatingSystem.lifecycle.ga
End-of-Life date	Nov-23-2013	operatingSystem.lifecycle.eol
End-of-Support date	Jun-18-2015	operatingSystem.lifecycle.eos

- The ‘lifecycle.stage’ token is useful when searching for the present stage of an asset.
- Use the other ‘lifecycle’ tokens to search for future EOL and EOS dates.

Software Lifecycle Search Tokens

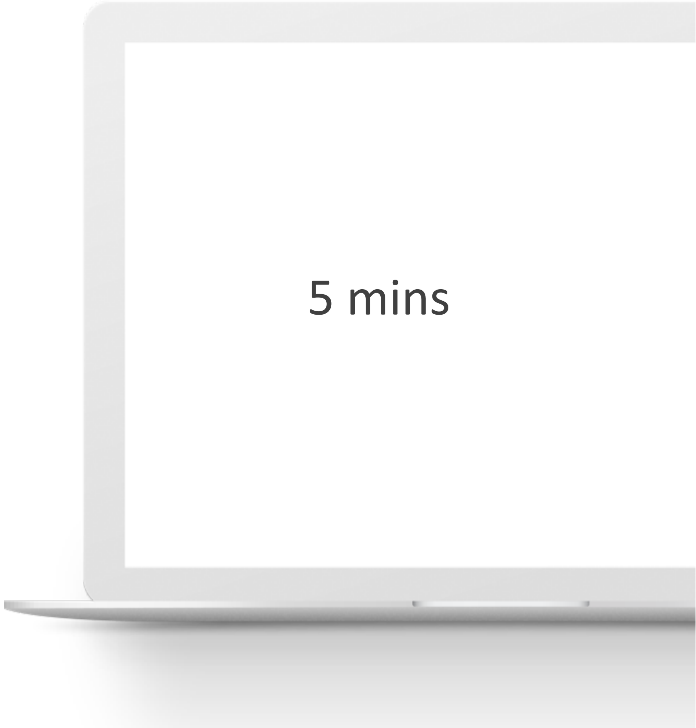
Attribute	Examples	Search Token
lifecycle stage	"Beta", "GA", "EOL", ”EOS"	software:(lifecycle.stage:
General Availability date	Apr-21-2014	software:(lifecycle.ga:
End-of-Life date	May-2016	software:(lifecycle.eol:
End-of-Support date	Jun-2018	software:(lifecycle.eos:

- The ‘lifecycle.stage’ token is useful when searching for the present stage of an asset.
- Use the other ‘lifecycle’ tokens to search for future EOL and EOS dates.

Lab 5 : Product Lifecycle Management

Please consult pages 23 to 24 in the lab tutorial supplement for details.

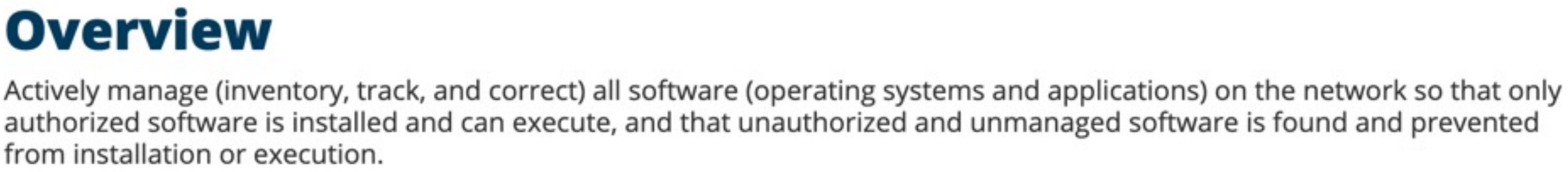
PLAY Tutorial begins on page 23.



5 mins

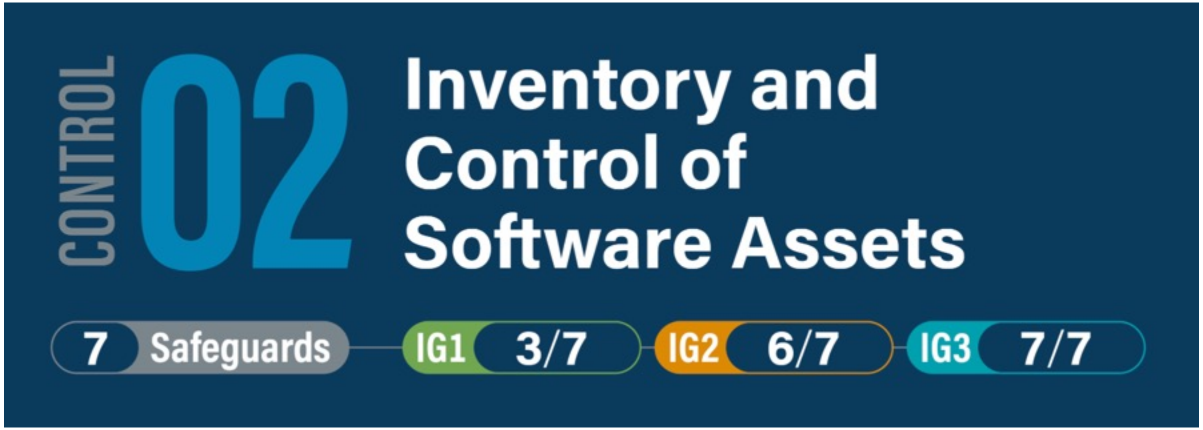
Authorized & Unauthorized Software

CIS Control 2: Inventory and Control of Software Assets



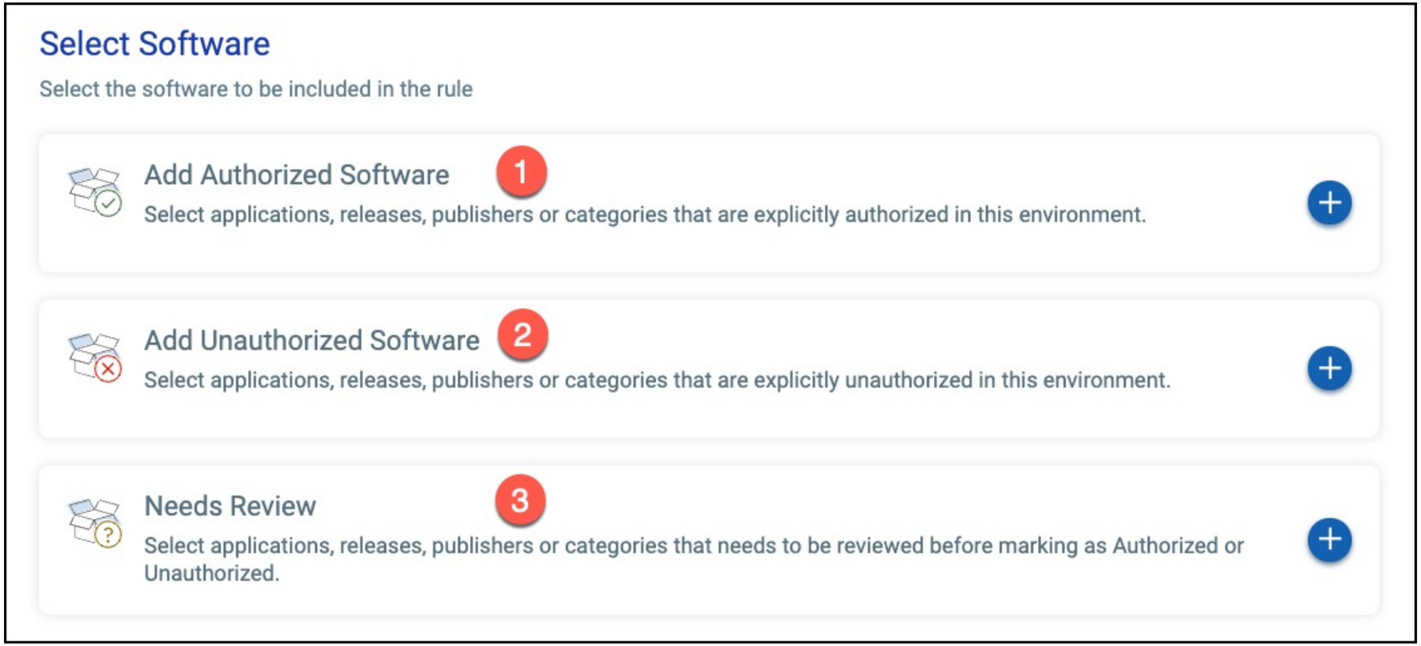
Overview

Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.



https://www.cisecurity.org/controls/inventory-and-control-of-software-assets/

Software Rule Types



Select Software

Select the software to be included in the rule

Add Authorized Software 1

Select applications, releases, publishers or categories that are explicitly authorized in this environment.

Add Unauthorized Software 2

Select applications, releases, publishers or categories that are explicitly unauthorized in this environment.

Needs Review 3

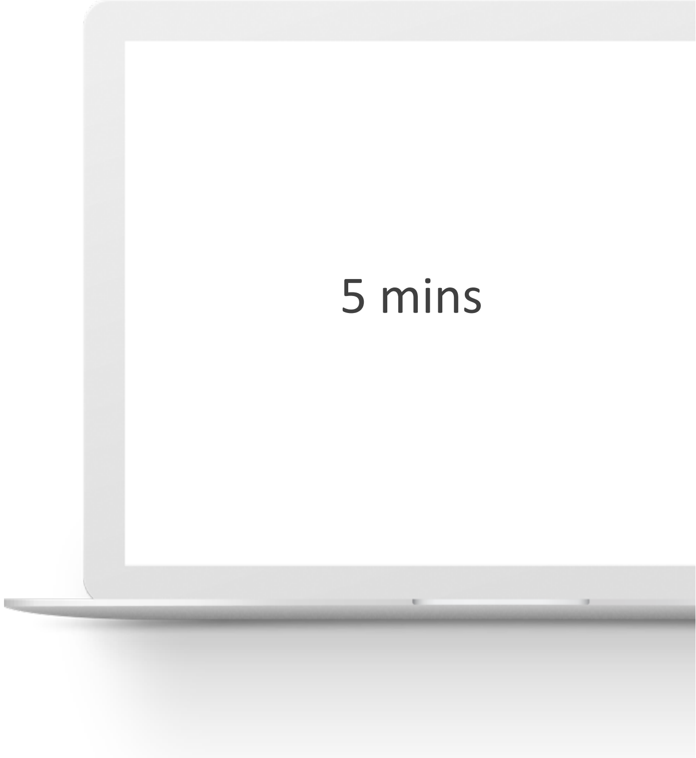
Select applications, releases, publishers or categories that needs to be reviewed before marking as Authorized or Unauthorized.

- Create rules for authorized/unauthorized software and software that needs to be reviewed.

Lab 6: Software Authorization

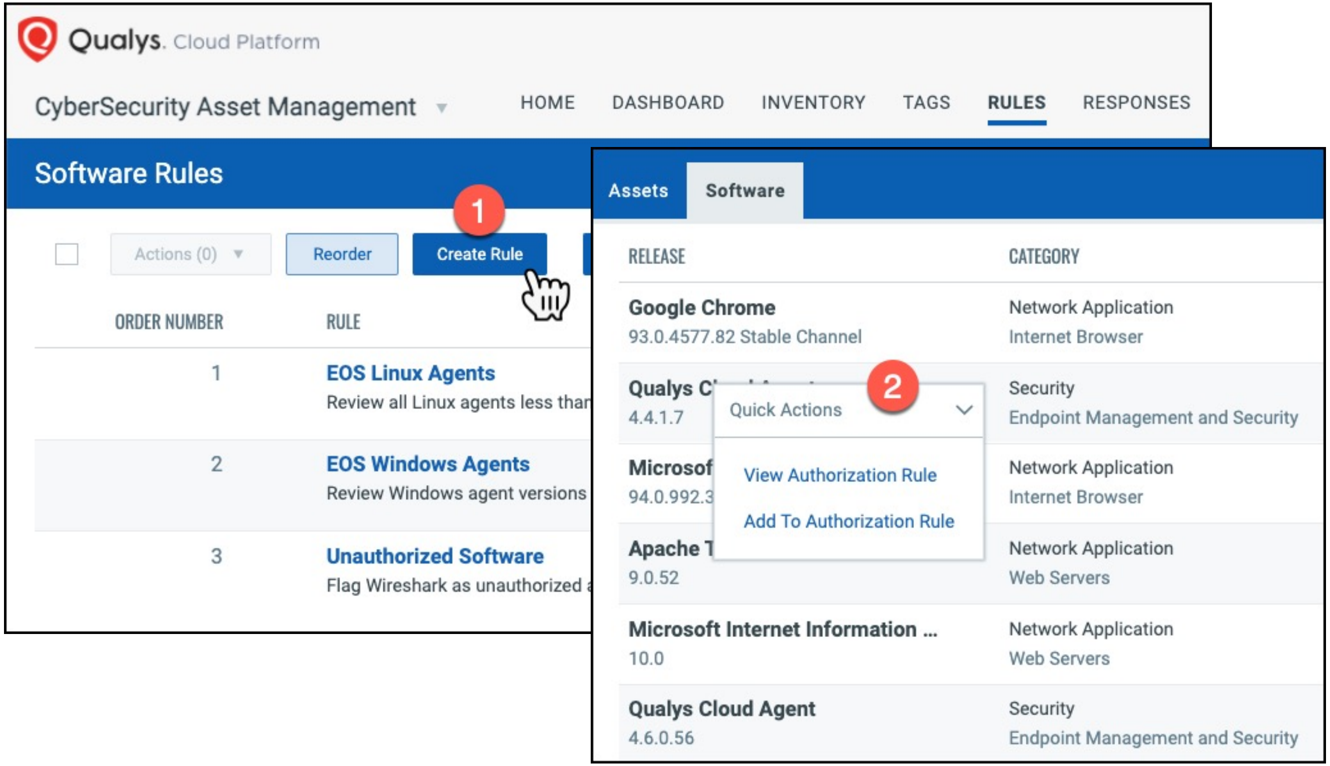
Please consult pages 25 - 27 in the lab tutorial supplement for details.

PLAY Tutorial begins on page 25.



5 mins

Create Software Rules

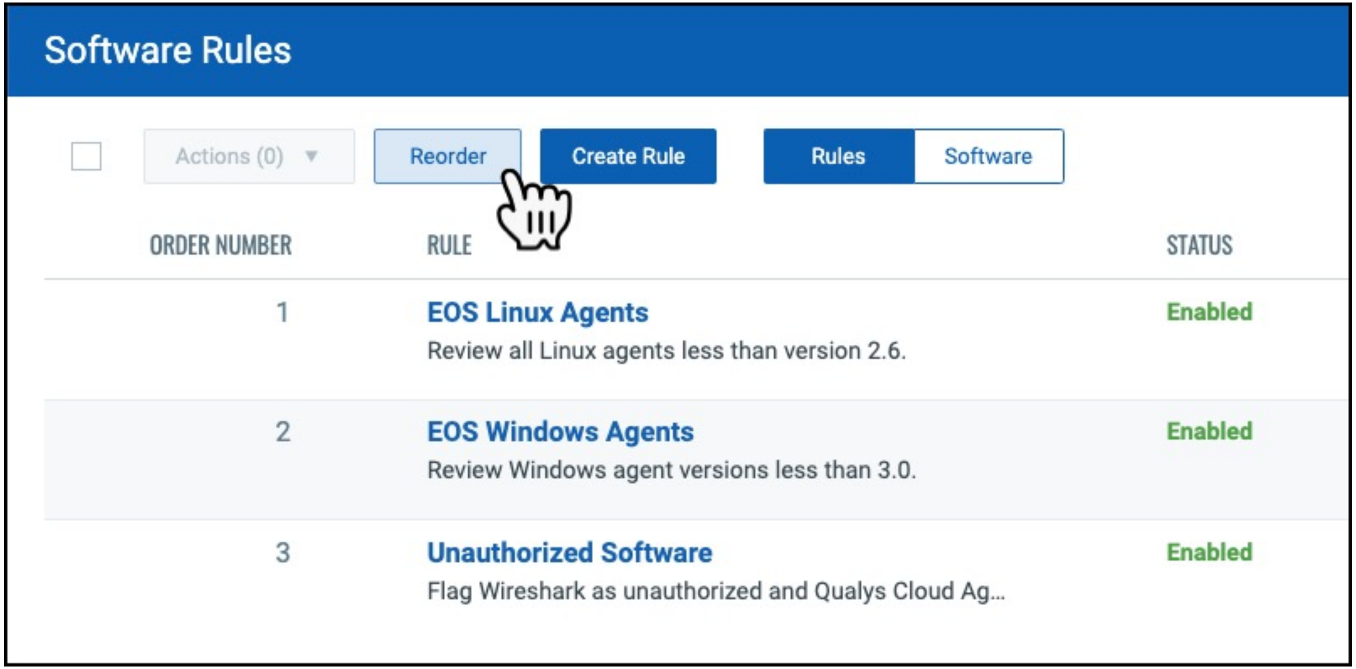


ORDER NUMBER	RULE
1	**EOS Linux Agents** Review all Linux agents less than
2	**EOS Windows Agents** Review Windows agent versions
3	**Unauthorized Software** Flag Wireshark as unauthorized a

RELEASE	CATEGORY
Google Chrome 93.0.4577.82 Stable Channel	Network Application Internet Browser
Qualys C 4.4.1.7	Security Endpoint Management and Security
Microsof 94.0.992.3	Network Application Internet Browser
Apache T 9.0.52	Network Application Web Servers
Microsoft Internet Information ... 10.0	Network Application Web Servers
Qualys Cloud Agent 4.6.0.56	Security Endpoint Management and Security

- View, create and modify rules from the RULES section or the “Software” tab under the INVENTORY section.

Rule Precedence



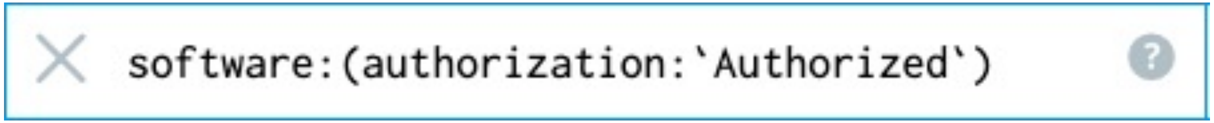
Software Rules

ORDER NUMBER	RULE	STATUS
1	**EOS Linux Agents** Review all Linux agents less than version 2.6.	Enabled
2	**EOS Windows Agents** Review Windows agent versions less than 3.0.	Enabled
3	**Unauthorized Software** Flag Wireshark as unauthorized and Qualys Cloud Ag...	Enabled

- Rules at the top of the list have precedence over the rules below.
- Click the “Reorder” button to move rules higher or lower.

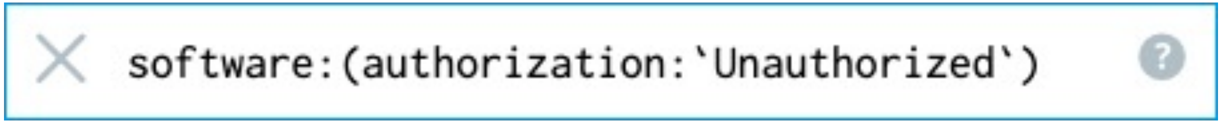
Software Authorization Tokens

- **AUTHORIZED**



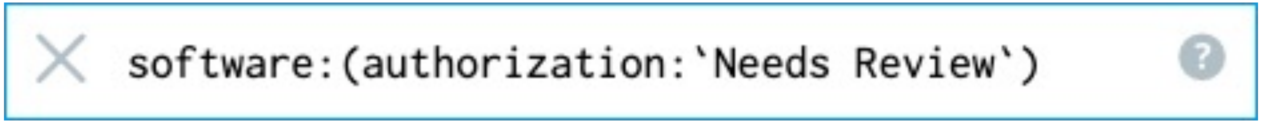
```
software:(authorization:`Authorized`)
```

- **UNAUTHORIZED**



```
software:(authorization:`Unauthorized`)
```

- **NEEDS REVIEW**



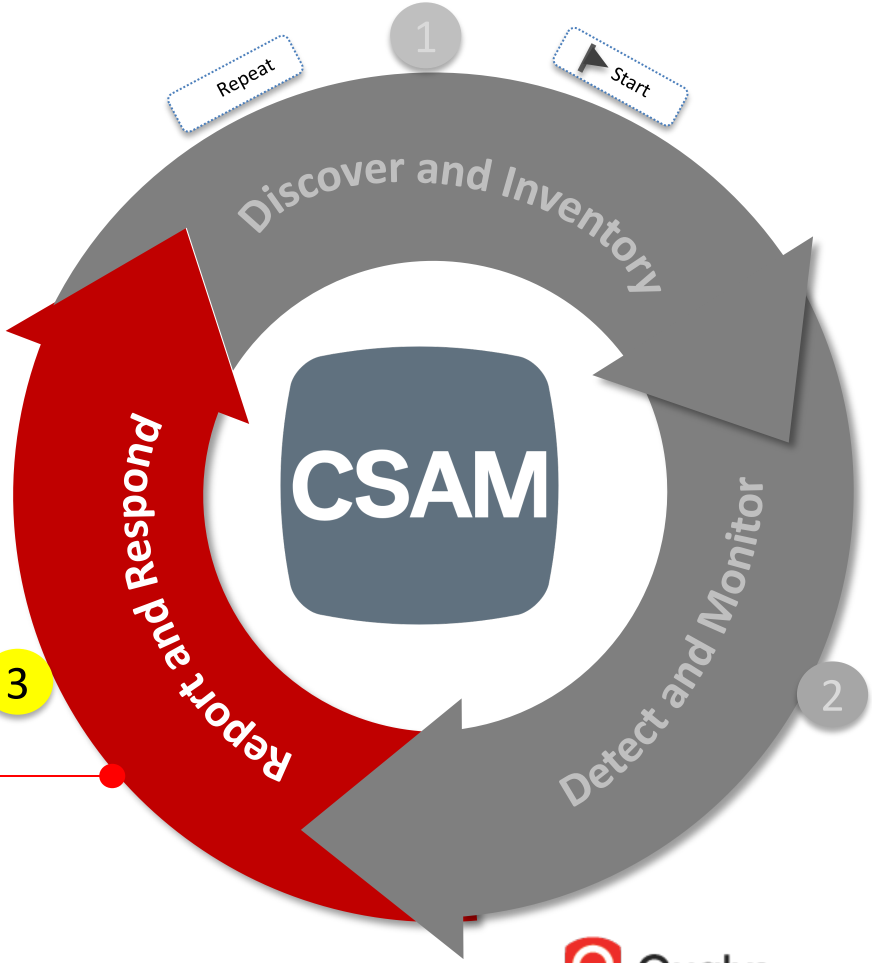
```
software:(authorization:`Needs Review`)
```

- After creating software authorization rules, software authorization tokens can be used to search and query.

Report & Respond

Report and Respond

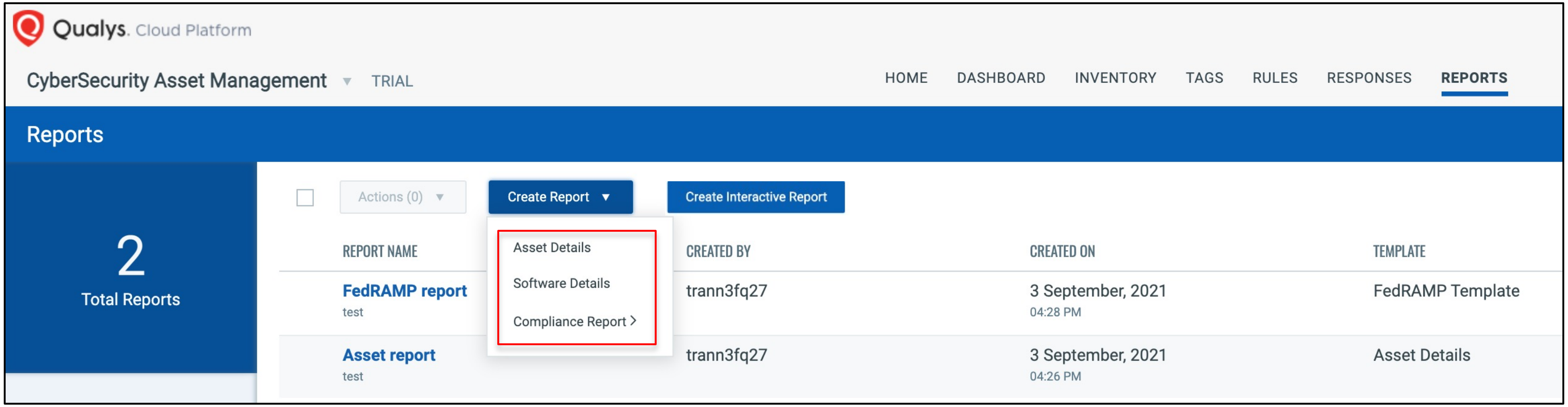
- **Visualize Data** (use dashboards to identify at risk assets)
- **Reports** (configure reports for IT and compliance requirements)*
- **Configure Rule-Based Alerts** (define criteria for alert notifications)*



Qualys.

Reports

Asset, Software and Compliance Reports



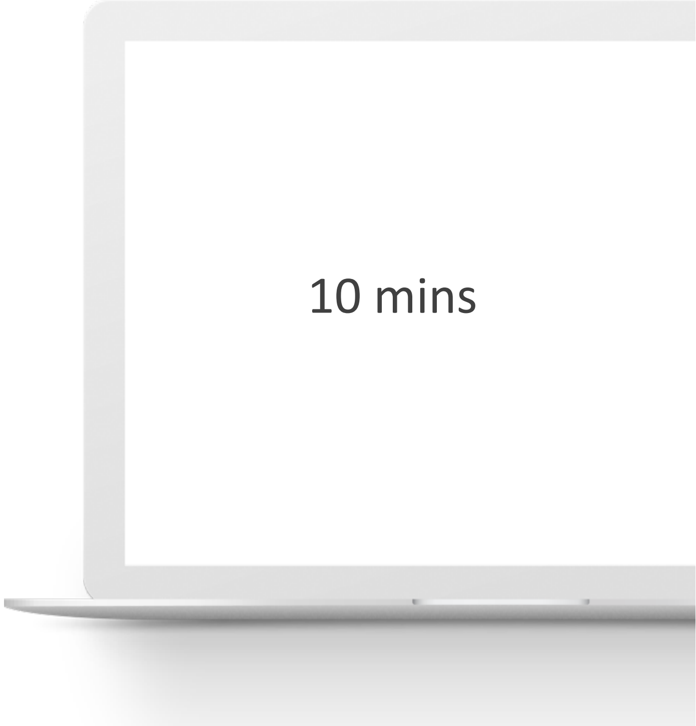
REPORT NAME	CREATED BY	CREATED ON	TEMPLATE
FedRAMP report test	trann3fq27	3 September, 2021 04:28 PM	FedRAMP Template
Asset report test	trann3fq27	3 September, 2021 04:26 PM	Asset Details

- Custom Reports (.csv file format)
  - Asset Details *(host information)*
  - Software Details *(host and software information)*
  - FedRAMP Compliance *(host and software information as required by RedRAMP)*

Lab 7 : Asset, Software, and Compliance Reports

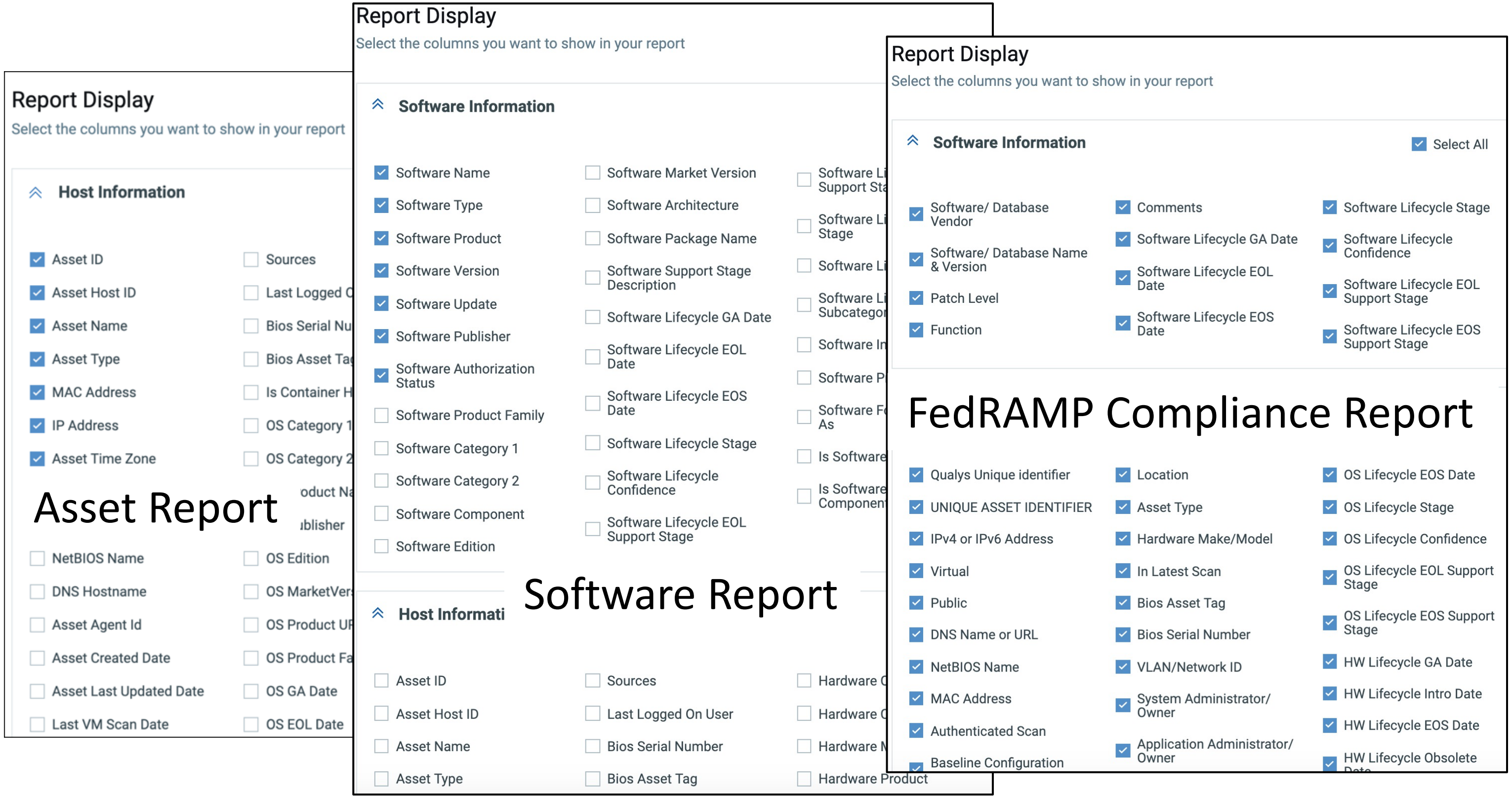
Please consult pages 28 to 30 in the lab tutorial supplement for details.

PLAY Tutorial begins on page 28.



10 mins

Display Options



Report Display

Select the columns you want to show in your report

Host Information

☑ Asset ID
☑ Asset Host ID
☑ Asset Name
☑ Asset Type
☑ MAC Address
☑ IP Address
☑ Asset Time Zone
□ NetBIOS Name
□ DNS Hostname
□ Asset Agent Id
□ Asset Created Date
□ Asset Last Updated Date
□ Last VM Scan Date

□ Sources
□ Last Logged O
□ Bios Serial Nu
□ Bios Asset Ta
□ Is Container H
□ OS Category 1
□ OS Category 2
oduct Na
ıblisher
□ OS Edition
□ OS MarketVer
□ OS Product UF
□ OS Product Fa
□ OS GA Date
□ OS EOL Date

Asset Report

Report Display

Select the columns you want to show in your report

Software Information

☑ Software Name
☑ Software Type
☑ Software Product
☑ Software Version
☑ Software Update
☑ Software Publisher
☑ Software Authorization Status
□ Software Product Family
□ Software Category 1
□ Software Category 2
□ Software Component
□ Software Edition

□ Software Market Version
□ Software Architecture
□ Software Package Name
□ Software Support Stage Description
□ Software Lifecycle GA Date
□ Software Lifecycle EOL Date
□ Software Lifecycle EOS Date
□ Software Lifecycle Stage
□ Software Lifecycle Confidence
□ Software Lifecycle EOL Support Stage

□ Software Li Support Sta
□ Software Li Stage
□ Software Li
□ Software Li Subcategor
□ Software In
□ Software P
□ Software Fo As
□ Is Software
□ Is Software Component

Host Informati

□ Asset ID
□ Asset Host ID
□ Asset Name
□ Asset Type

□ Sources
□ Last Logged On User
□ Bios Serial Number
□ Bios Asset Tag

□ Hardware C
□ Hardware C
□ Hardware M
□ Hardware Product

Software Report

Report Display

Select the columns you want to show in your report

Software Information ☑ Select All

☑ Software/ Database Vendor
☑ Software/ Database Name & Version
☑ Patch Level
☑ Function

☑ Comments
☑ Software Lifecycle GA Date
☑ Software Lifecycle EOL Date
☑ Software Lifecycle EOS Date

☑ Software Lifecycle Stage
☑ Software Lifecycle Confidence
☑ Software Lifecycle EOL Support Stage
☑ Software Lifecycle EOS Support Stage

FedRAMP Compliance Report

☑ Qualys Unique identifier
☑ UNIQUE ASSET IDENTIFIER
☑ IPv4 or IPv6 Address
☑ Virtual
☑ Public
☑ DNS Name or URL
☑ NetBIOS Name
☑ MAC Address
☑ Authenticated Scan
☑ Baseline Configuration

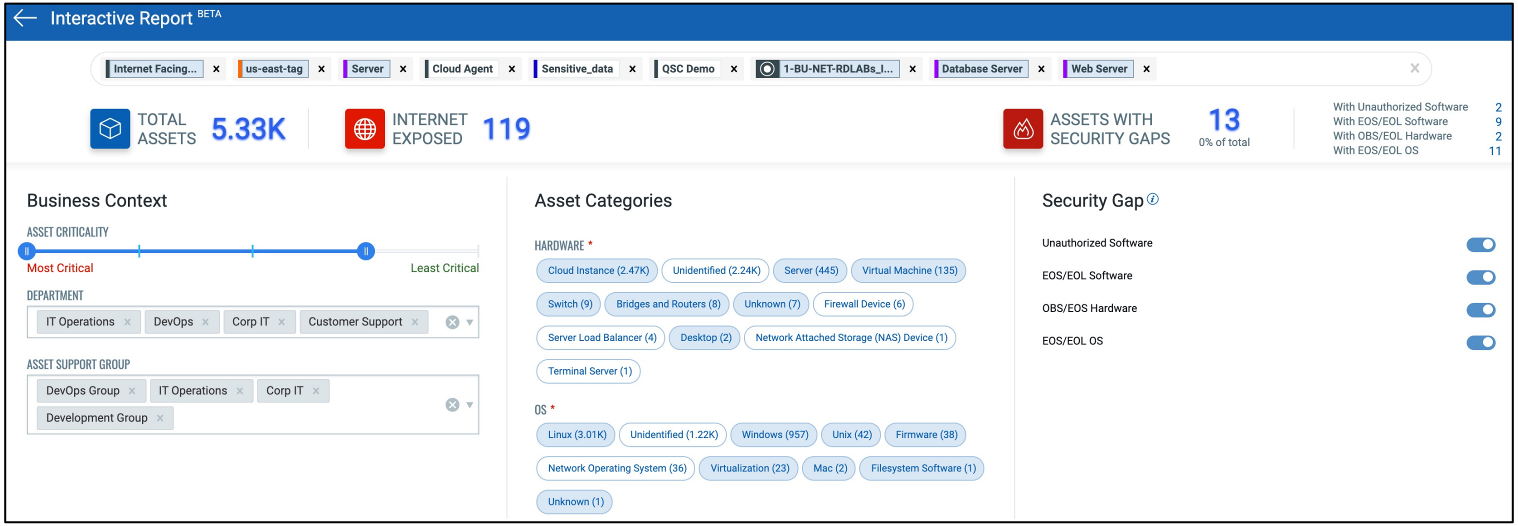
☑ Location
☑ Asset Type
☑ Hardware Make/Model
☑ In Latest Scan
☑ Bios Asset Tag
☑ Bios Serial Number
☑ VLAN/Network ID
☑ System Administrator/ Owner
☑ Application Administrator/ Owner

☑ OS Lifecycle EOS Date
☑ OS Lifecycle Stage
☑ OS Lifecycle Confidence
☑ OS Lifecycle EOL Support Stage
☑ OS Lifecycle EOS Support Stage
☑ HW Lifecycle GA Date
☑ HW Lifecycle Intro Date
☑ HW Lifecycle EOS Date
☑ HW Lifecycle Obsolete Date

Selected attributes will be column headers in the report

Qualys.

Interactive Report



Interactive Report BETA

Internet Facing... × | us-east-tag × | Server × | Cloud Agent × | Sensitive_data × | QSC Demo × | 1-BU-NET-RDLABs_I... × | Database Server × | Web Server ×

TOTAL ASSETS 5.33K

INTERNET EXPOSED 119

ASSETS WITH SECURITY GAPS 13
0% of total

With Unauthorized Software	2
With EOS/EOL Software	9
With OBS/EOL Hardware	2
With EOS/EOL OS	11

Business Context

ASSET CRITICALITY

Most Critical — Least Critical

DEPARTMENT

IT Operations × | DevOps × | Corp IT × | Customer Support ×

ASSET SUPPORT GROUP

DevOps Group × | IT Operations × | Corp IT × | Development Group ×

Asset Categories

HARDWARE *

Cloud Instance (2.47K) | Unidentified (2.24K) | Server (445) | Virtual Machine (135) | Switch (9) | Bridges and Routers (8) | Unknown (7) | Firewall Device (6) | Server Load Balancer (4) | Desktop (2) | Network Attached Storage (NAS) Device (1) | Terminal Server (1)

OS *

Linux (3.01K) | Unidentified (1.22K) | Windows (957) | Unix (42) | Firmware (38) | Network Operating System (36) | Virtualization (23) | Mac (2) | Filesystem Software (1) | Unknown (1)

Security Gap

Unauthorized Software ●

EOS/EOL Software ●

OBS/EOS Hardware ●

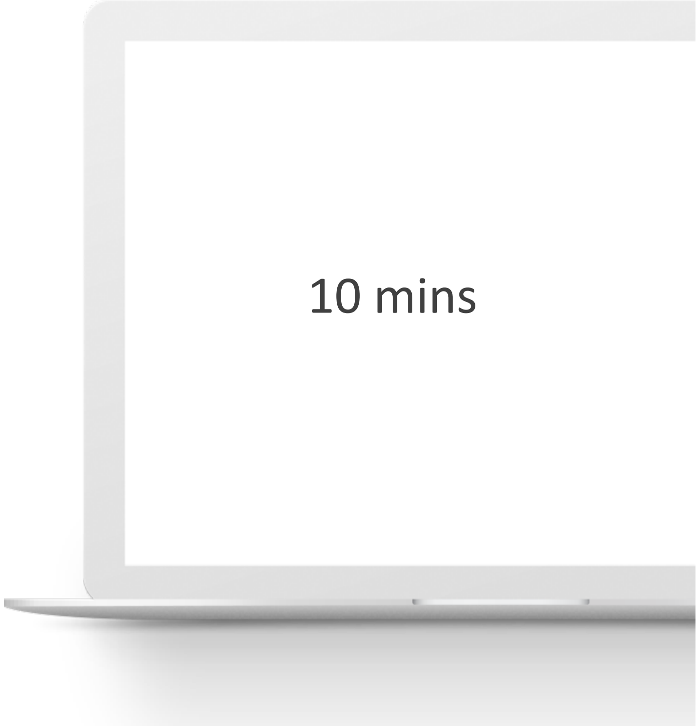
EOS/EOL OS ●

- Includes an interactive workflow to identify and list issues and security gaps (obsolete hardware, EOL/EOS software, unauthorized software, etc.).

Lab 8 : Interactive Reports

Please consult pages 31 to 33 in the lab tutorial supplement for details.

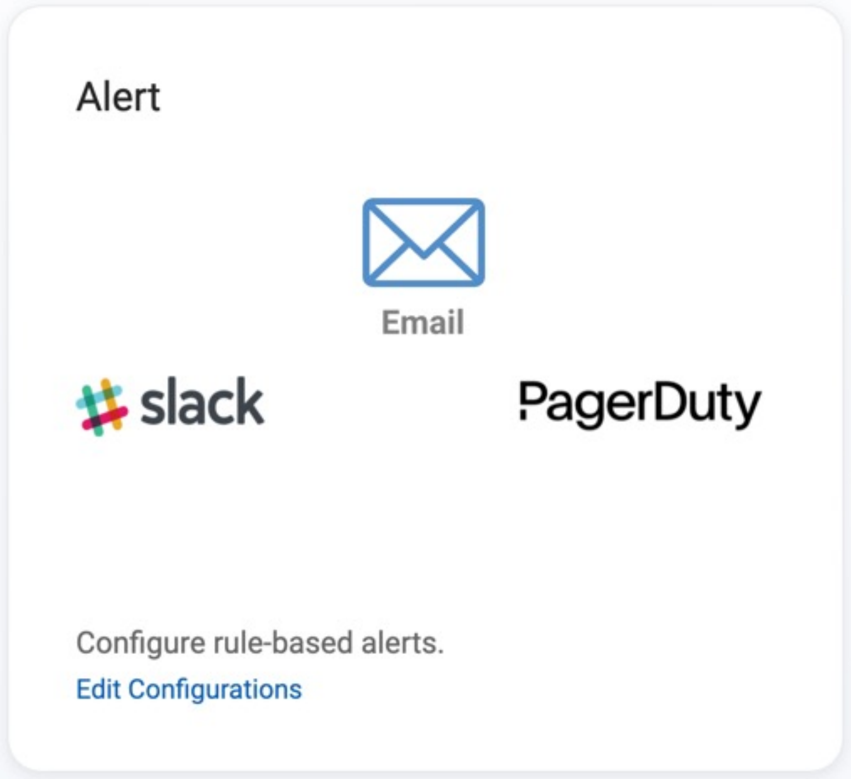
PLAY Tutorial begins on page 31.



10 mins

Rule-Based Alerts

Alert Actions



Alert

Configure rule-based alerts.

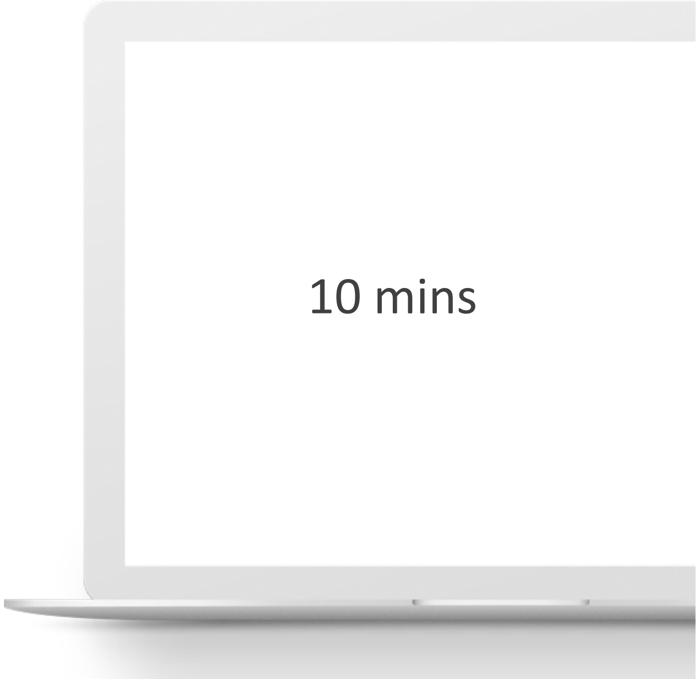
Edit Configurations

- Receive alert notifications via Email, Slack, and PagerDuty.
- Alert Rules are evaluated when host inventory is updated.
- One or more actions must be defined prior to creating Alert Rules.

Lab 9 : Rule-Based Alerts

Please consult pages 34 to 37 in the lab tutorial supplement for details.

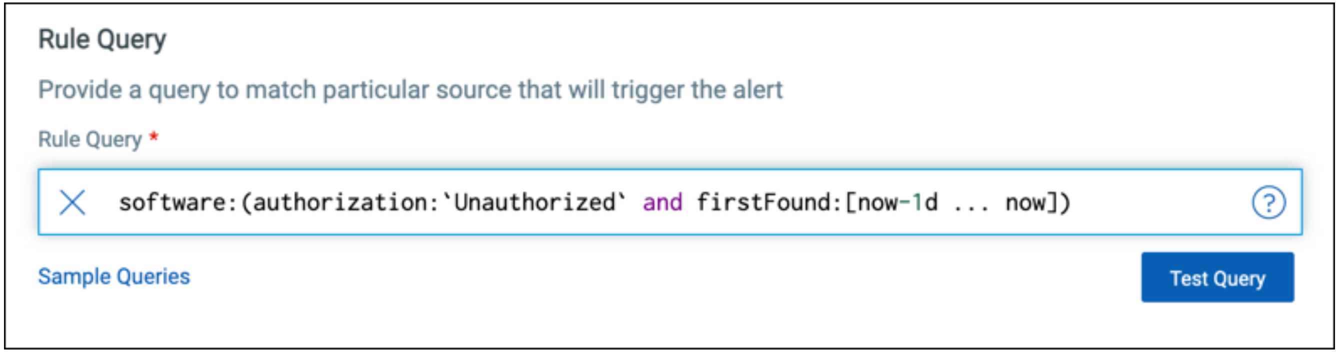
PLAY Tutorial begins on page 34.



10 mins

Rule Query

- The Rule Query specifies the criteria for triggering an alert action.



Rule Query

Provide a query to match particular source that will trigger the alert

Rule Query *

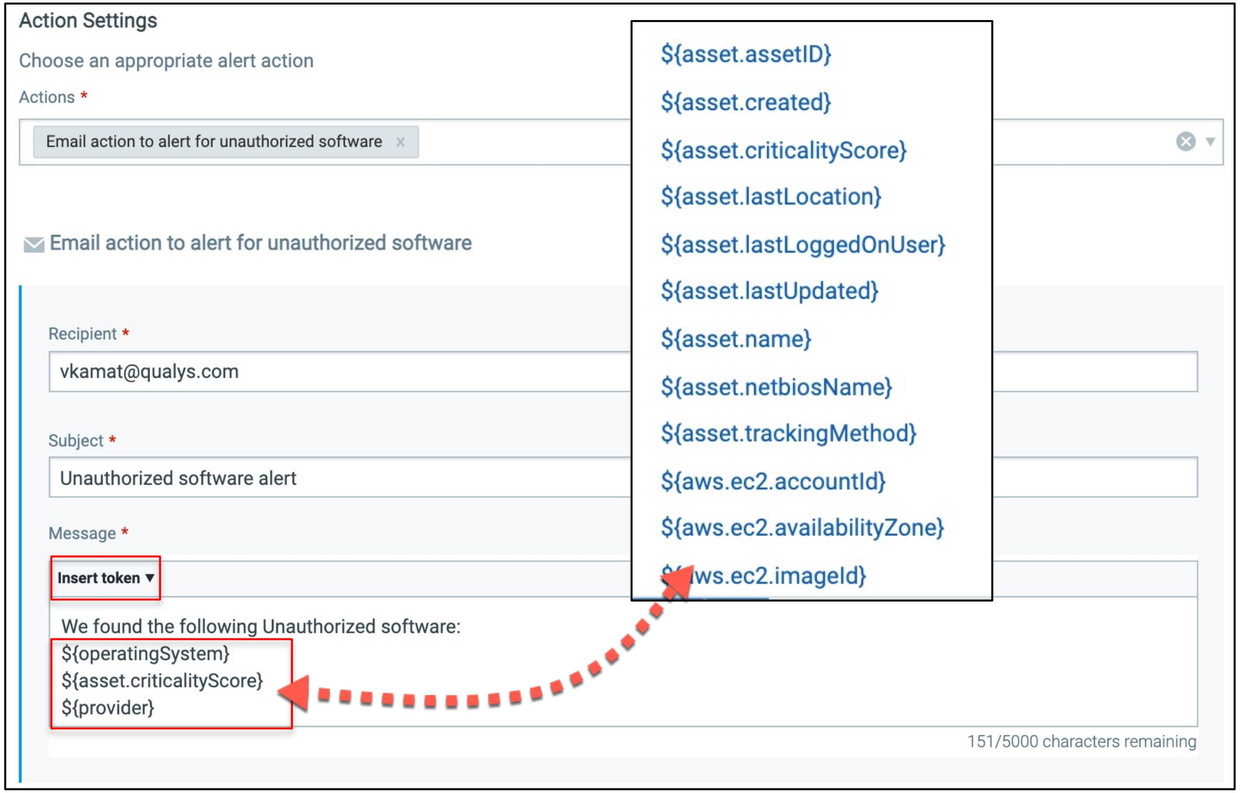
```
software:(authorization:`Unauthorized` and firstFound:[now-1d ... now])
```

- Sample queries are provided to get you started.
- Immediately notify your operational teams when critical or suspicious events are monitored:
  - Unauthorized software discovered
  - Assets reaching EOS dates
  - Insufficient storage space on host
  - Malicious software discovered
  - and more...

Insert Tokens

Insert tokens into the message body to include useful asset information and details in the alert:

- Asset Criticality Score
- Last Logged On User
- AWS, Azure, and GCP metadata
- Hardware and OS categories
- and more...



Action Settings

Choose an appropriate alert action

Actions *

Email action to alert for unauthorized software

Email action to alert for unauthorized software

Recipient *

vkamat@qualys.com

Subject *

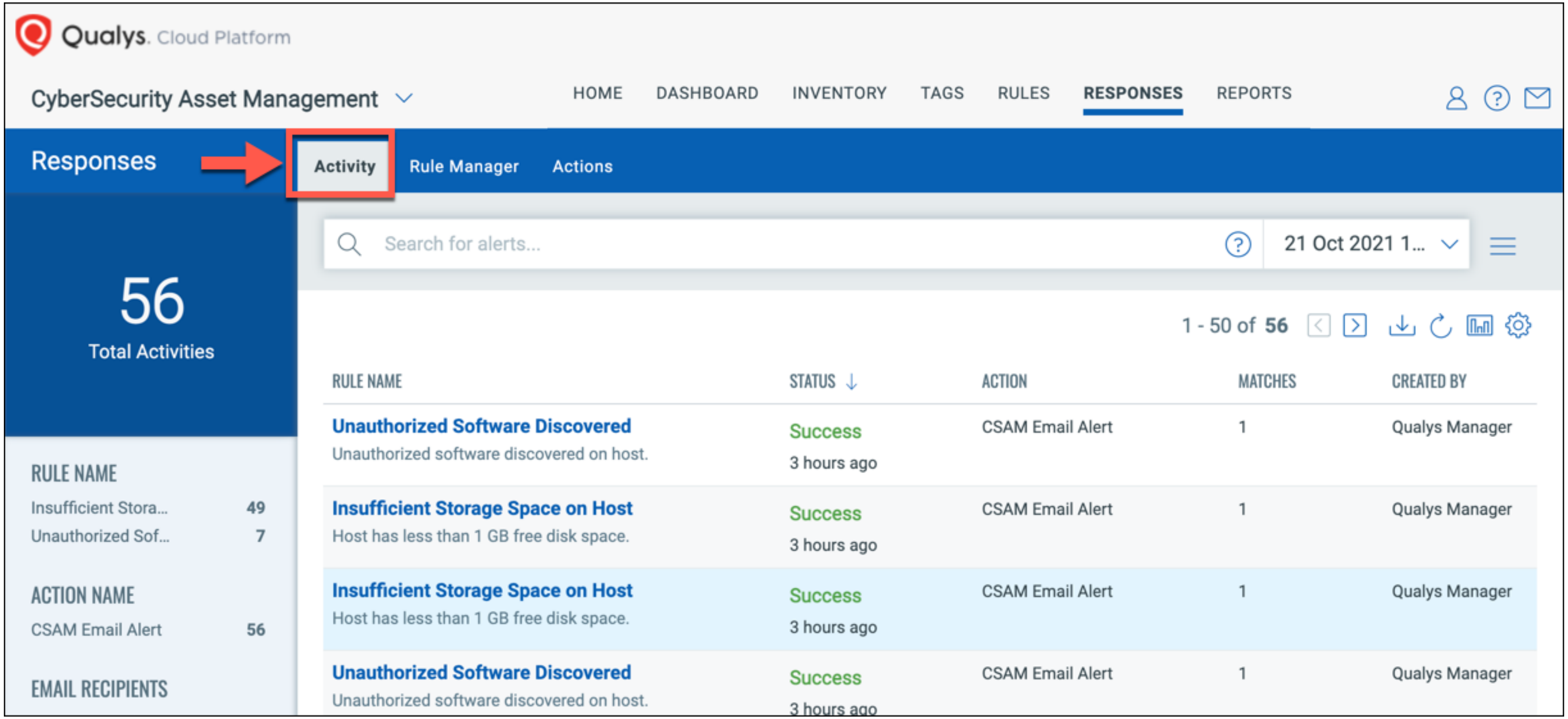
Unauthorized software alert

Message *

We found the following Unauthorized software:
${operatingSystem}
${asset.criticalityScore}
${provider}

151/5000 characters remaining

Alert Activity



56
Total Activities

RULE NAME

Insufficient Stora...	49
Unauthorized Sof...	7

ACTION NAME

CSAM Email Alert	56

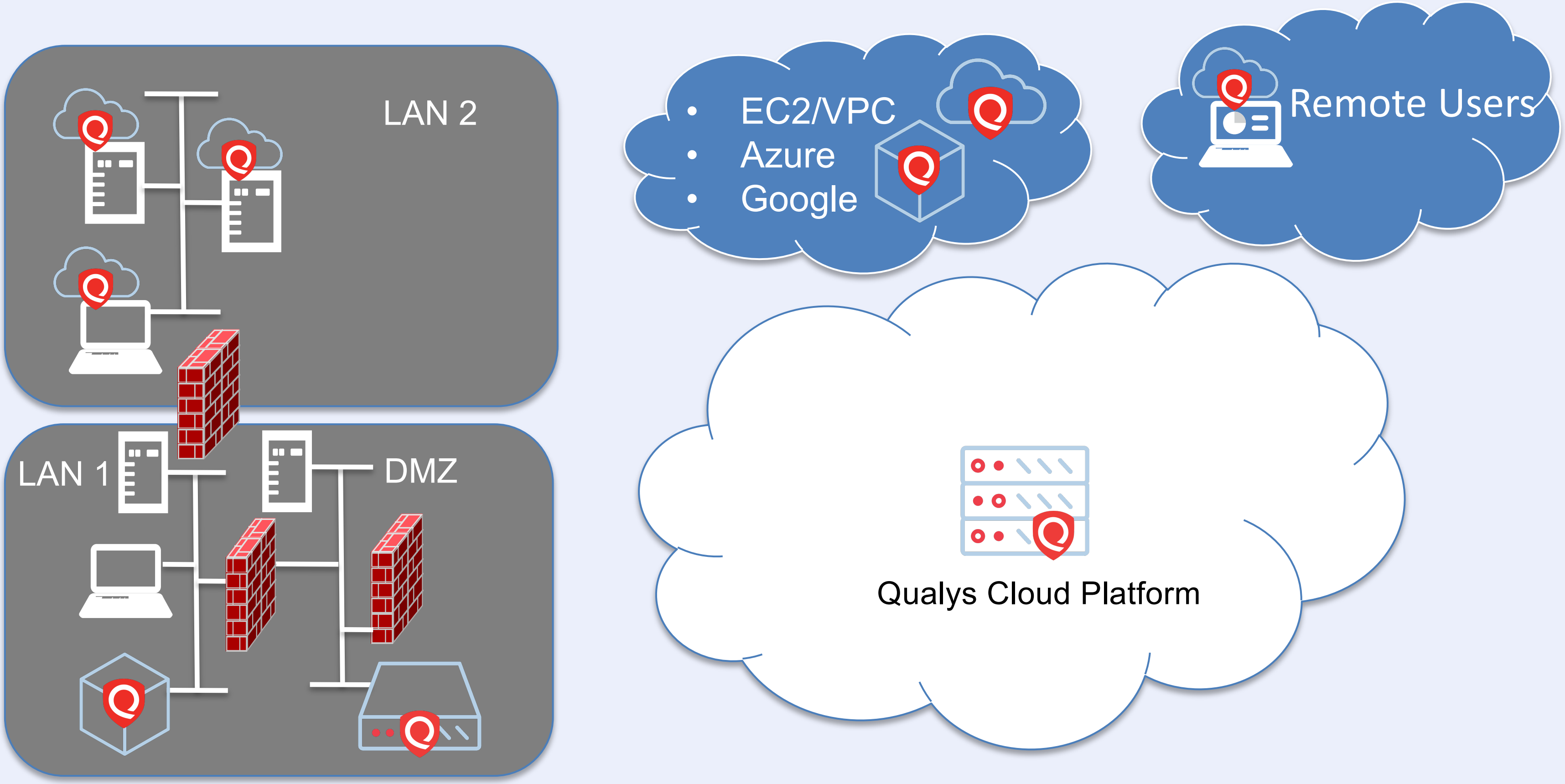
EMAIL RECIPIENTS

RULE NAME	STATUS ↓	ACTION	MATCHES	CREATED BY
Unauthorized Software Discovered Unauthorized software discovered on host.	Success 3 hours ago	CSAM Email Alert	1	Qualys Manager
Insufficient Storage Space on Host Host has less than 1 GB free disk space.	Success 3 hours ago	CSAM Email Alert	1	Qualys Manager
Insufficient Storage Space on Host Host has less than 1 GB free disk space.	Success 3 hours ago	CSAM Email Alert	1	Qualys Manager
Unauthorized Software Discovered Unauthorized software discovered on host.	Success 3 hours ago	CSAM Email Alert	1	Qualys Manager

- Monitor alert activity under the “Activity” tab.

Vulnerability Management

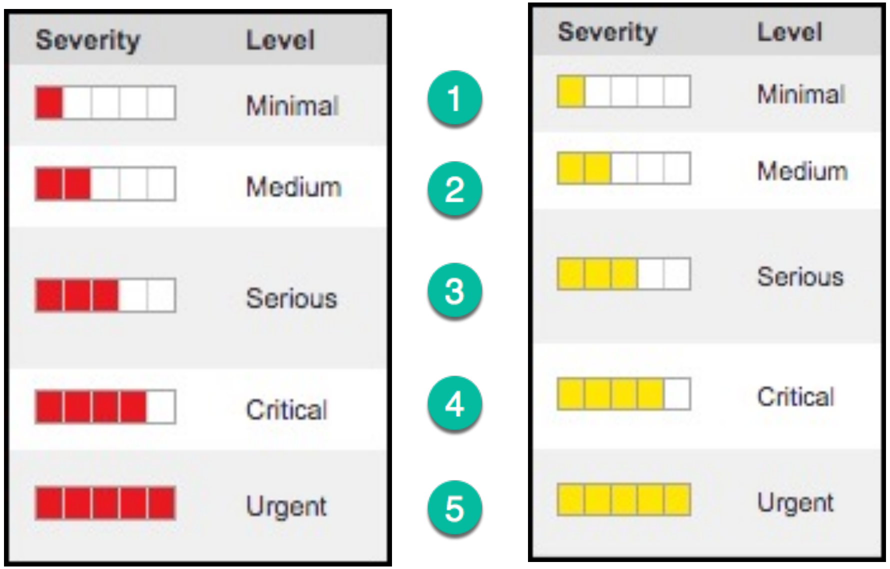
VM Sensors


LAN 2
LAN 1
DMZ
EC2/VPC
Azure
Google
Remote Users
Qualys Cloud Platform

Vulnerability Findings

- Industry-leading vulnerability KnowledgeBase with tens-of-thousands of vulnerability signatures.

- Each vulnerability is ranked and associated with:
  - Qualys Severity Level
  - CVSS Score
  - CVE & Bugtraq IDs
  - Available Patches
  - Known Threats
  - Associated Malware
  - and more...



Severity	Level		Severity	Level
🟥⬜⬜⬜⬜	Minimal	1	🟨⬜⬜⬜⬜	Minimal
🟥🟥⬜⬜⬜	Medium	2	🟨🟨⬜⬜⬜	Medium
🟥🟥🟥⬜⬜	Serious	3	🟨🟨🟨⬜⬜	Serious
🟥🟥🟥🟥⬜	Critical	4	🟨🟨🟨🟨⬜	Critical
🟥🟥🟥🟥🟥	Urgent	5	🟨🟨🟨🟨🟨	Urgent

- An unlimited number of ways to identify, prioritize, and patch vulnerabilities.

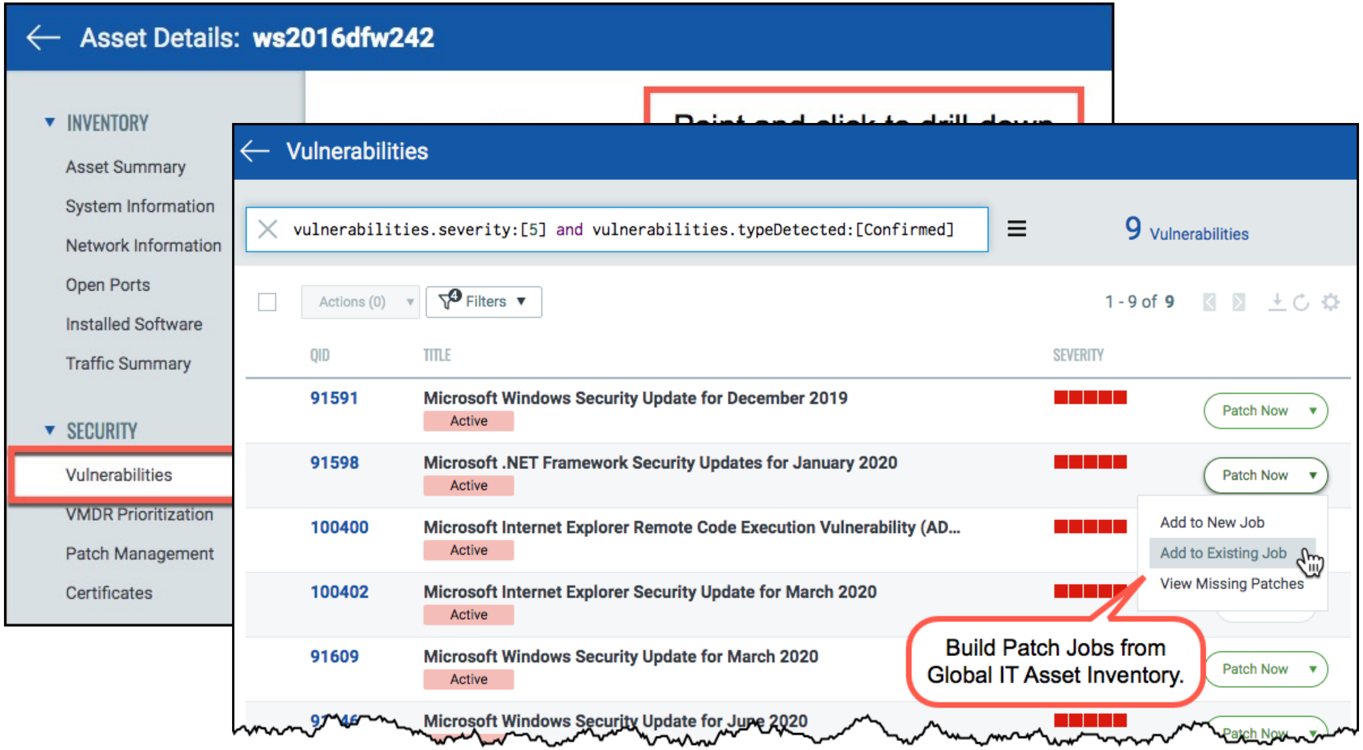
Lab 10 : Vulnerability Findings

Please consult pages 38 to 40 in the lab tutorial supplement for details.

PLAY Tutorial begins on page 39.

5 mins

Vulnerability Findings In CSAM



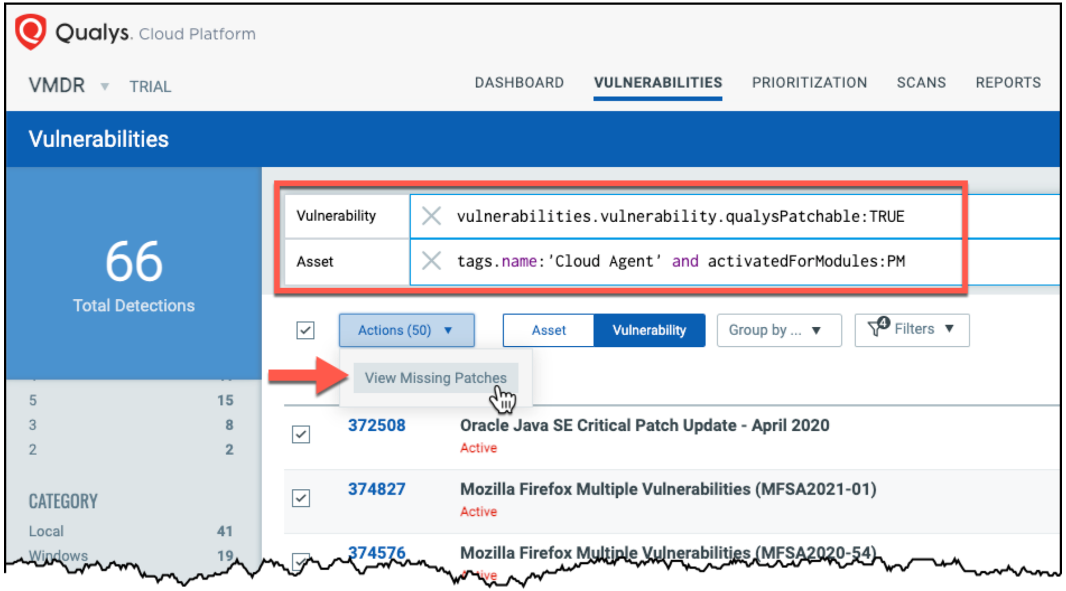
```
vulnerabilities.severity:[5] and vulnerabilities.typeDetected:[Confirmed]
```

QID	TITLE	SEVERITY
91591	Microsoft Windows Security Update for December 2019 Active	🟥🟥🟥🟥🟥
91598	Microsoft .NET Framework Security Updates for January 2020 Active	🟥🟥🟥🟥🟥
100400	Microsoft Internet Explorer Remote Code Execution Vulnerability (AD... Active	🟥🟥🟥🟥🟥
100402	Microsoft Internet Explorer Security Update for March 2020 Active	🟥🟥🟥🟥🟥
91609	Microsoft Windows Security Update for March 2020 Active	
91646	Microsoft Windows Security Update for June 2020	🟥🟥🟥🟥🟥

Build Patch Jobs from Global IT Asset Inventory.

- View and patch vulnerability findings from within CyberSecurity Asset Management (on a per asset basis).

Vulnerability Findings in VMDR



Vulnerability	vulnerabilities.vulnerability.qualysPatchable:TRUE
Asset	tags.name:'Cloud Agent' and activatedForModules:PM

5	15
3	8
2	2
Local	41
Windows	19

☑	372508	Oracle Java SE Critical Patch Update - April 2020 Active
☑	374827	Mozilla Firefox Multiple Vulnerabilities (MFSA2021-01) Active
☑	374576	Mozilla Firefox Multiple Vulnerabilities (MFSA2020-54) Active

Which ones are patchable?

1. Detected vulnerabilities must be associated with one or more patches found in the Qualys Patch Catalog

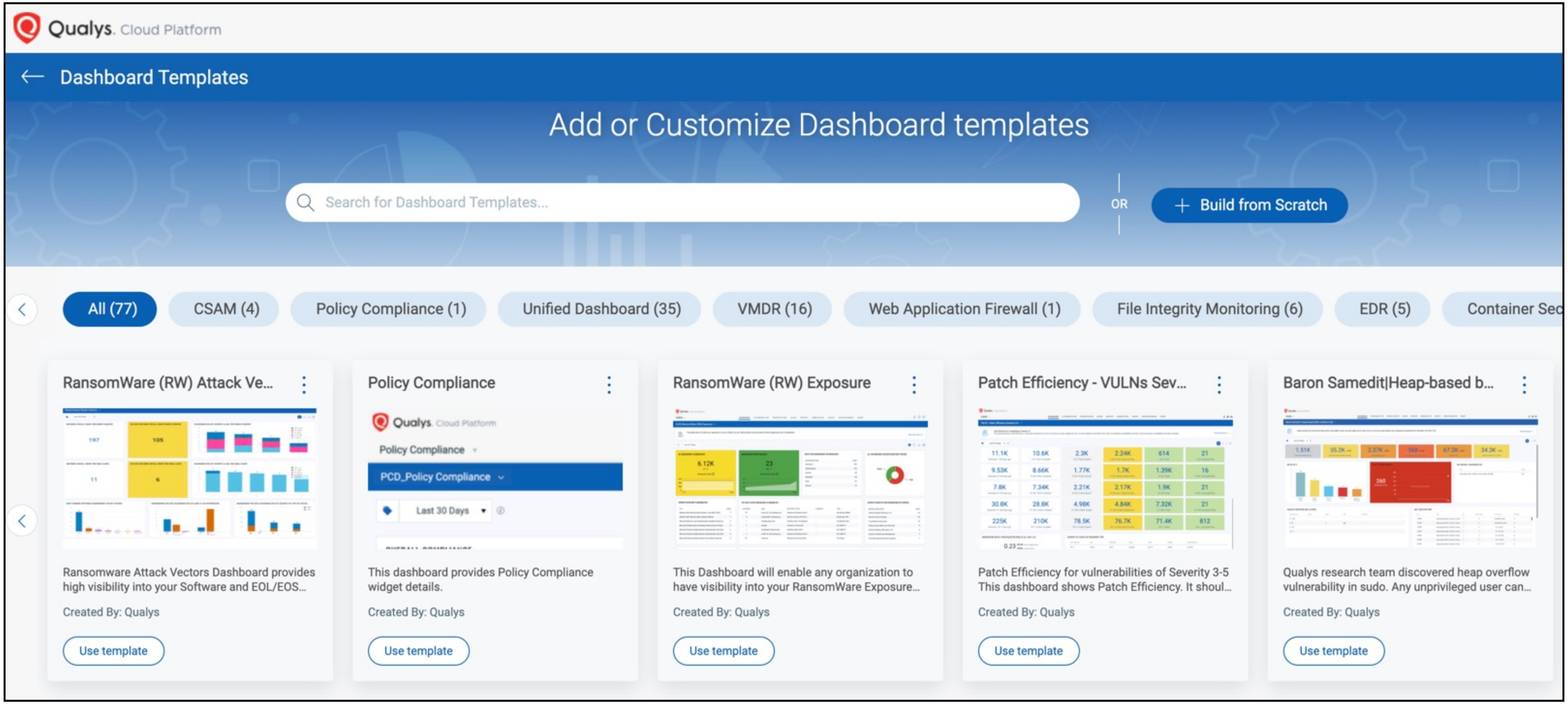
2. Detection Host must be running the Qualys Cloud Agent

3. Cloud Agent must have the PM module activated

Dashboards & Widgets

Qualys.

Out-of-Box Dashboard Templates



Qualys. Cloud Platform

← Dashboard Templates

Add or Customize Dashboard templates

Search for Dashboard Templates...

OR

+ Build from Scratch

All (77) | CSAM (4) | Policy Compliance (1) | Unified Dashboard (35) | VMDR (16) | Web Application Firewall (1) | File Integrity Monitoring (6) | EDR (5) | Container Sec

RansomWare (RW) Attack Ve...

Ransomware Attack Vectors Dashboard provides high visibility into your Software and EOL/EOS...

Created By: Qualys

Use template

Policy Compliance

This dashboard provides Policy Compliance widget details.

Created By: Qualys

Use template

RansomWare (RW) Exposure

This Dashboard will enable any organization to have visibility into your RansomWare Exposure...

Created By: Qualys

Use template

Patch Efficiency - VULNs Sev...

Patch Efficiency for vulnerabilities of Severity 3-5 This dashboard shows Patch Efficiency. It shoul...

Created By: Qualys

Use template

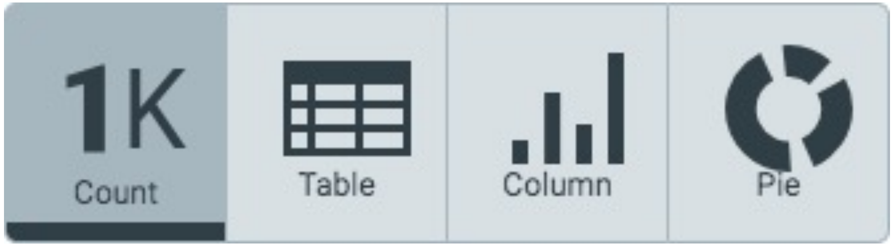
Baron Samedit|Heap-based b...

Qualys research team discovered heap overflow vulnerability in sudo. Any unprivileged user can...

Created By: Qualys

Use template

Widget Types



Dashboard widgets can be designed to display query results as counts, tables, columns, or pie charts.

Lab 11 : Dashboards & Widgets

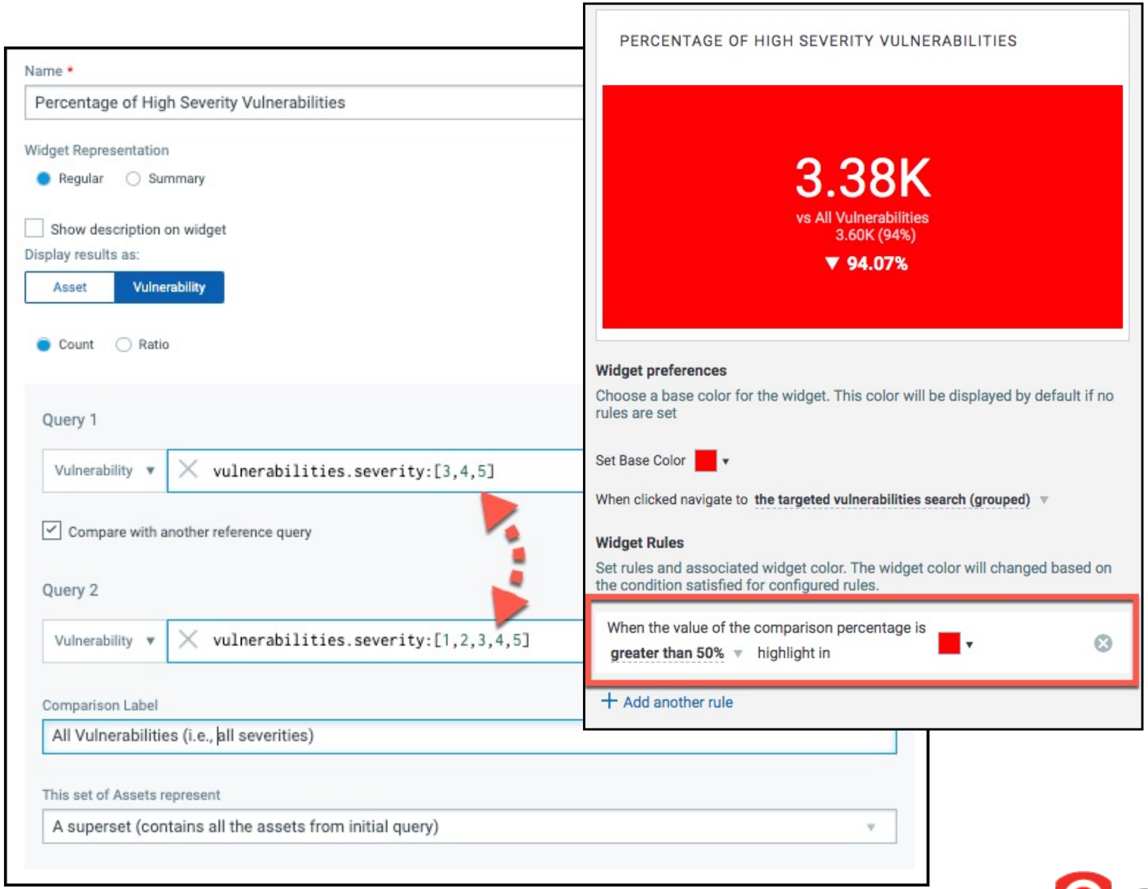
Please consult pages 41 to 44 in the lab tutorial supplement for details.

PLAY Tutorial begins on page 41.

5 mins

Count Widget

- The “Count Widget” can be configured to automatically change color, when specific conditions or thresholds are met.



Name *

Percentage of High Severity Vulnerabilities

Widget Representation

● Regular ○ Summary

□ Show description on widget

Display results as:

Asset | **Vulnerability**

● Count ○ Ratio

Query 1

Vulnerability ▾ | vulnerabilities.severity:[3,4,5]

☑ Compare with another reference query

Query 2

Vulnerability ▾ | vulnerabilities.severity:[1,2,3,4,5]

Comparison Label

All Vulnerabilities (i.e., all severities)

This set of Assets represent

A superset (contains all the assets from initial query) ▾

PERCENTAGE OF HIGH SEVERITY VULNERABILITIES

3.38K

vs All Vulnerabilities
3.60K (94%)

▼ 94.07%

Widget preferences

Choose a base color for the widget. This color will be displayed by default if no rules are set

Set Base Color 🟥 ▾

When clicked navigate to **the targeted vulnerabilities search (grouped)** ▾

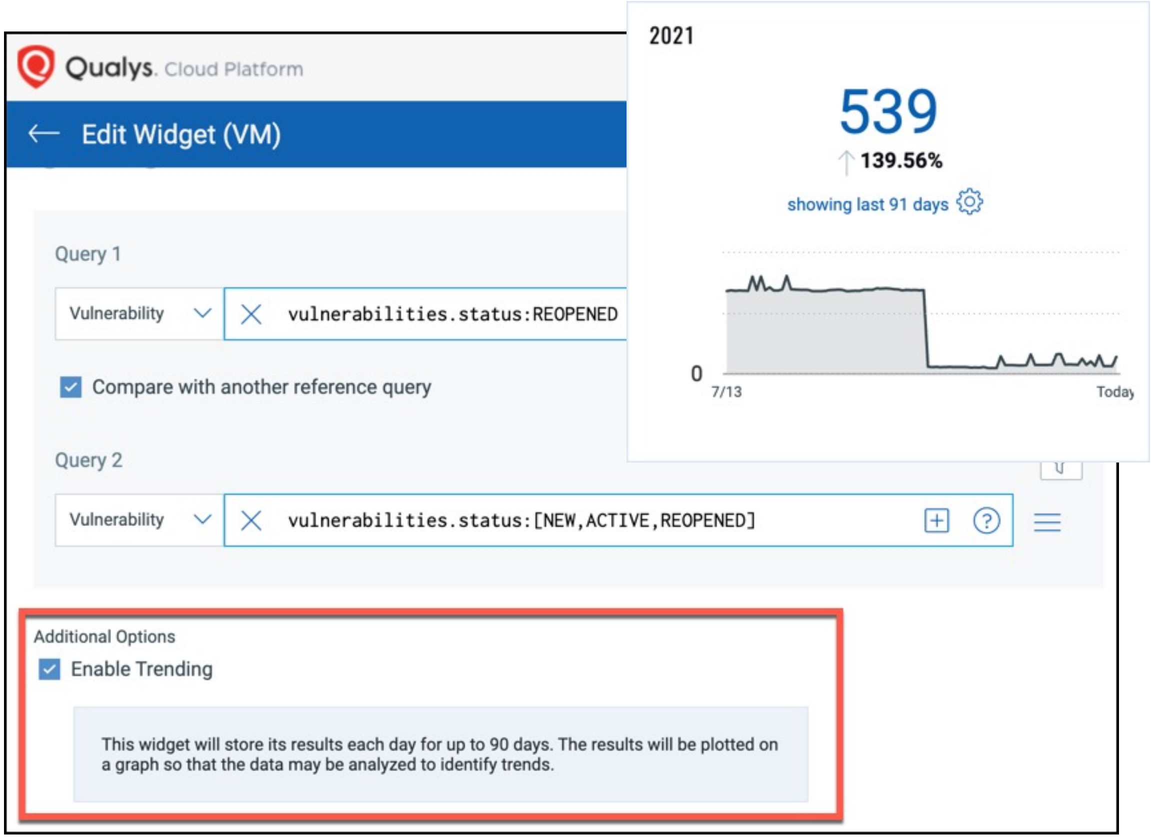
Widget Rules

Set rules and associated widget color. The widget color will changed based on the condition satisfied for configured rules.

When the value of the comparison percentage is **greater than 50%** ▾ highlight in 🟥 ▾

+ Add another rule

Enable Trending in Widgets



Query 1

Vulnerability | vulnerabilities.status:REOPENED

☑ Compare with another reference query

Query 2

Vulnerability | vulnerabilities.status:[NEW,ACTIVE,REOPENED]

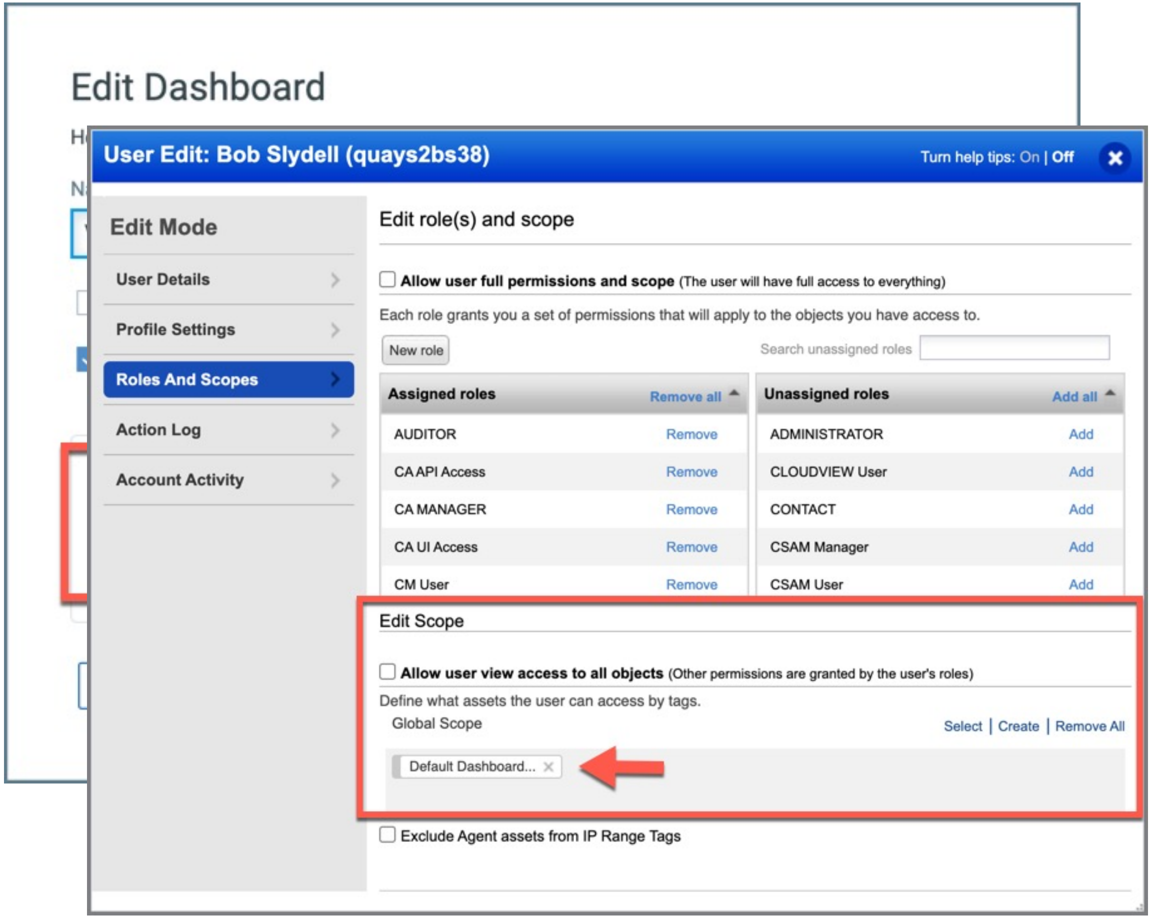
Additional Options

☑ Enable Trending

This widget will store its results each day for up to 90 days. The results will be plotted on a graph so that the data may be analyzed to identify trends.

- Visualize changes or swings in momentum or progress.
- When enabled, widgets can store trend data for up to 90 days.
- Trend lines plotted on a graph are added to the widget.

Dashboard Tags



Edit Dashboard

User Edit: Bob Slydell (quays2bs38) Turn help tips: On | Off ✕

Edit Mode

- User Details
- Profile Settings
- **Roles And Scopes**
- Action Log
- Account Activity

Edit role(s) and scope

□ **Allow user full permissions and scope** (The user will have full access to everything)

Each role grants you a set of permissions that will apply to the objects you have access to.

New role Search unassigned roles

Assigned roles	Remove all	Unassigned roles	Add all
AUDITOR	Remove	ADMINISTRATOR	Add
CA API Access	Remove	CLOUDVIEW User	Add
CA MANAGER	Remove	CONTACT	Add
CA UI Access	Remove	CSAM Manager	Add
CM User	Remove	CSAM User	Add

Edit Scope

□ **Allow user view access to all objects** (Other permissions are granted by the user's roles)

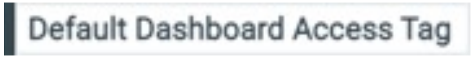
Define what assets the user can access by tags.

Global Scope Select | Create | Remove All

Default Dashboard... ✕

□ Exclude Agent assets from IP Range Tags

- Add one or more Asset Tags through the Dashboard Editor.
- The “Default Dashboard Access Tag” is created by Qualys.

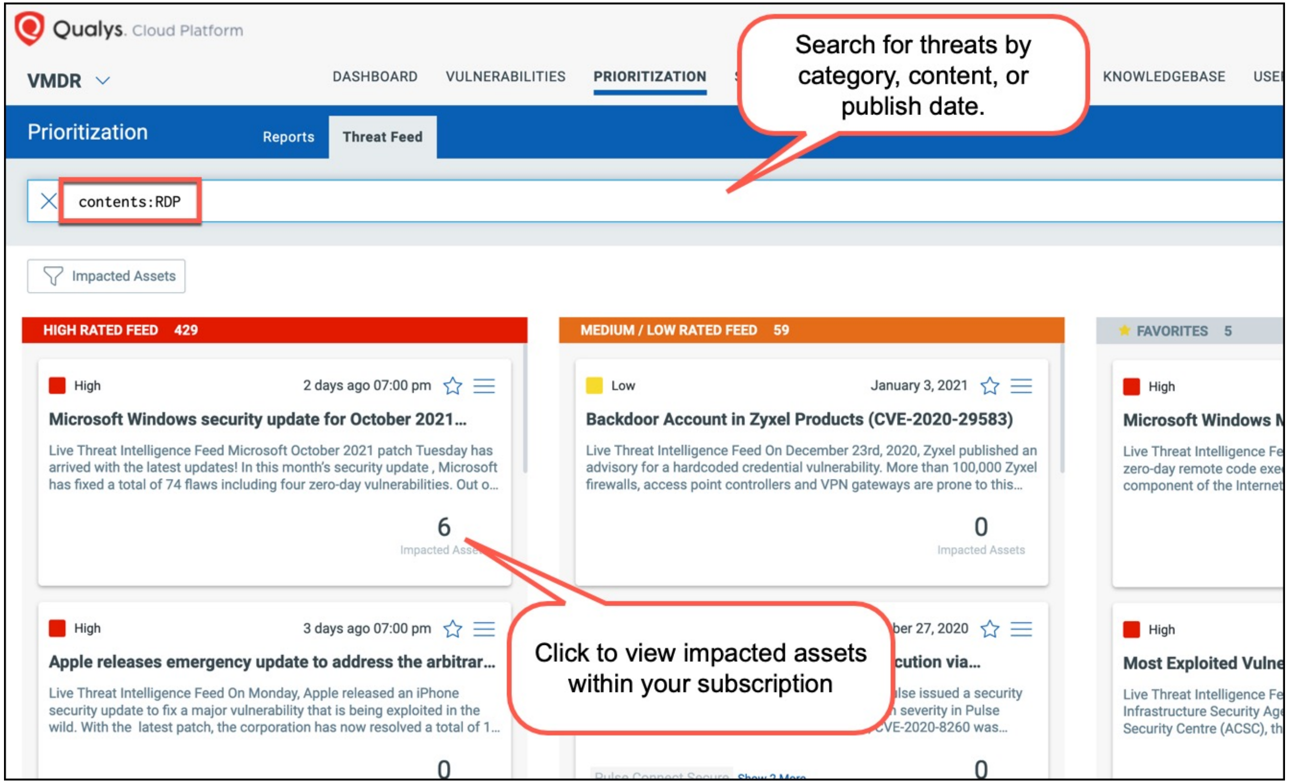


Default Dashboard Access Tag

- Share dashboards with other Qualys users by assigning “dashboard” tag(s) to their accounts.

Threat Detection & Prioritization

VMDR Threat Feed



contents:RDP

Search for threats by category, content, or publish date.

High 2 days ago 07:00 pm

Microsoft Windows security update for October 2021...

Live Threat Intelligence Feed Microsoft October 2021 patch Tuesday has arrived with the latest updates! In this month's security update , Microsoft has fixed a total of 74 flaws including four zero-day vulnerabilities. Out o...

6 Impacted Asse

Low January 3, 2021

Backdoor Account in Zyxel Products (CVE-2020-29583)

Live Threat Intelligence Feed On December 23rd, 2020, Zyxel published an advisory for a hardcoded credential vulnerability. More than 100,000 Zyxel firewalls, access point controllers and VPN gateways are prone to this...

0 Impacted Assets

High

Microsoft Windows M

Live Threat Intelligence Fe zero-day remote code exe component of the Internet

High 3 days ago 07:00 pm

Apple releases emergency update to address the arbitrar...

Live Threat Intelligence Feed On Monday, Apple released an iPhone security update to fix a major vulnerability that is being exploited in the wild. With the latest patch, the corporation has now resolved a total of 1...

0

ber 27, 2020

cution via...

lse issued a security n severity in Pulse CVE-2020-8260 was...

Pulse Connect Secure Show 2 More

0

High

Most Exploited Vulne

Live Threat Intelligence Fe Infrastructure Security Ag Security Centre (ACSC), th

Click to view impacted assets within your subscription

Search for threats by content, category or publish date and click to view impacted assets.

Threat Feed Sources

Exploit Sources

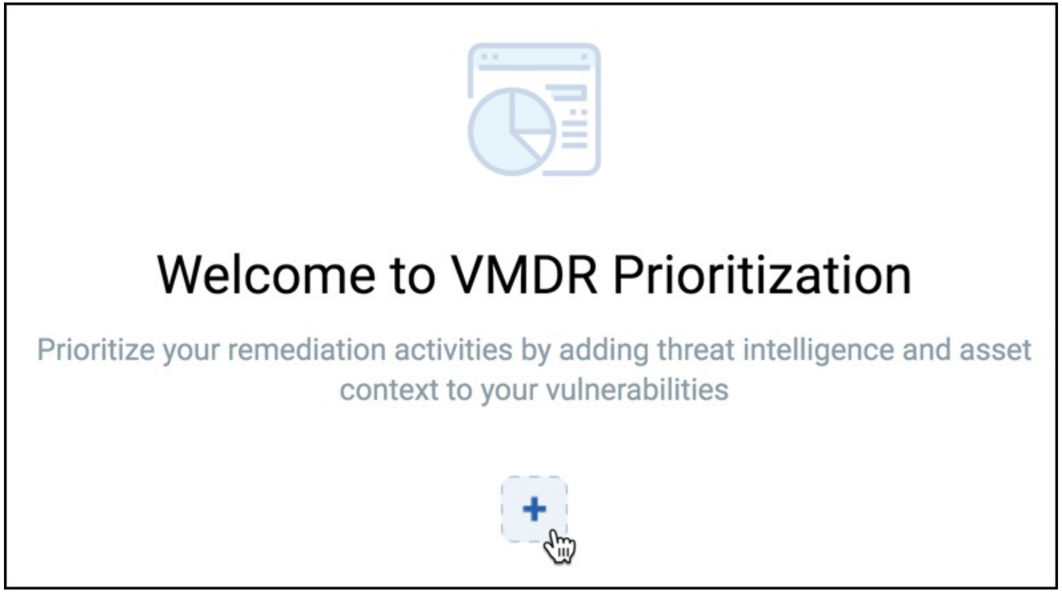
Source Type	Data Type
Core Security	PoC Exploits mapped to CVEs
Exploit-DB	PoC Exploits mapped to CVEs
Metasploit	PoC Exploits mapped to CVEs
Contagio Dump	Exploit Kits mapped to CVEs
Immunity - Agora - Dsquare - Enable Security - White Phosporus	PoC Exploits mapped to CVEs
Google Project Zero	Zero-Days mapped to CVEs

Malware Sources

Source Type	Data Type
Reversing Labs	CVEs associated with malware
Trend Micro	Malware names associated with CVEs
McAfee	Ransomware mapped to CVEs

- The Qualys Threat and Malware research team leverages exploit and malware data from multiple sources.

VMDR Prioritization Report



Welcome to VMDR Prioritization

Prioritize your remediation activities by adding threat intelligence and asset context to your vulnerabilities

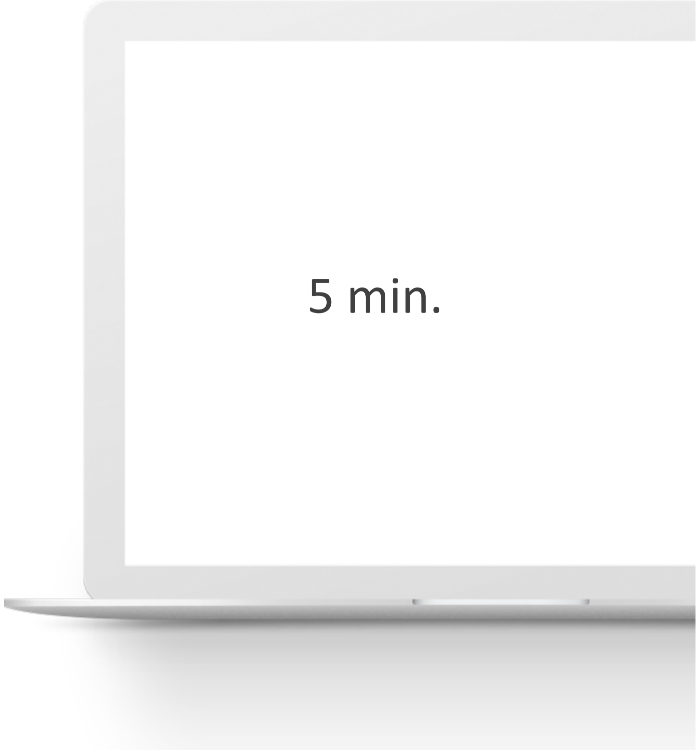
Prioritize vulnerabilities by:

- Asset Context
- Vulnerability Age
- Threat Intelligence
- Attack Surface

Lab 12: VMDR Prioritization Report

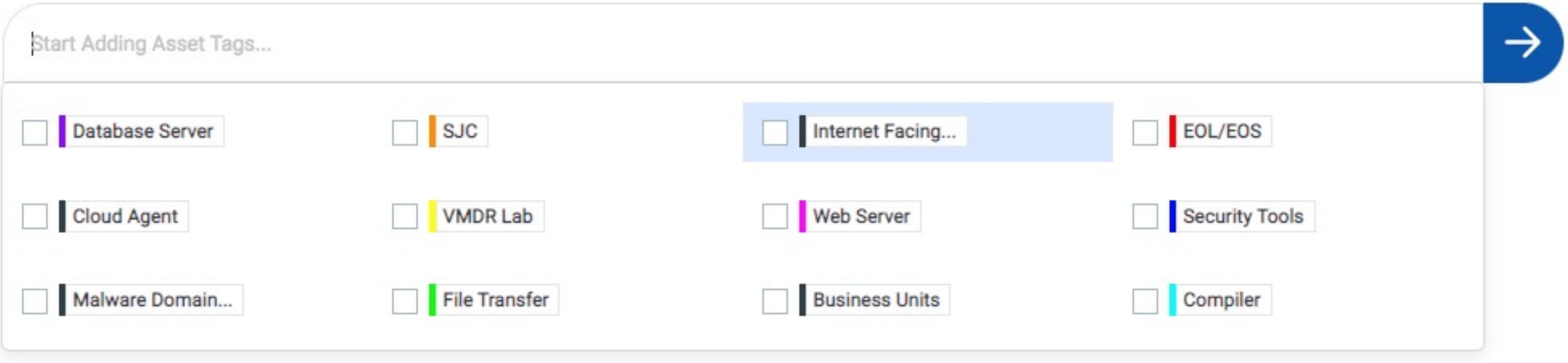
Please consult pages 46 to 51 in the lab tutorial supplement for details.

PLAY Tutorial begins on page 46.



5 min.

Asset Tags Add Context

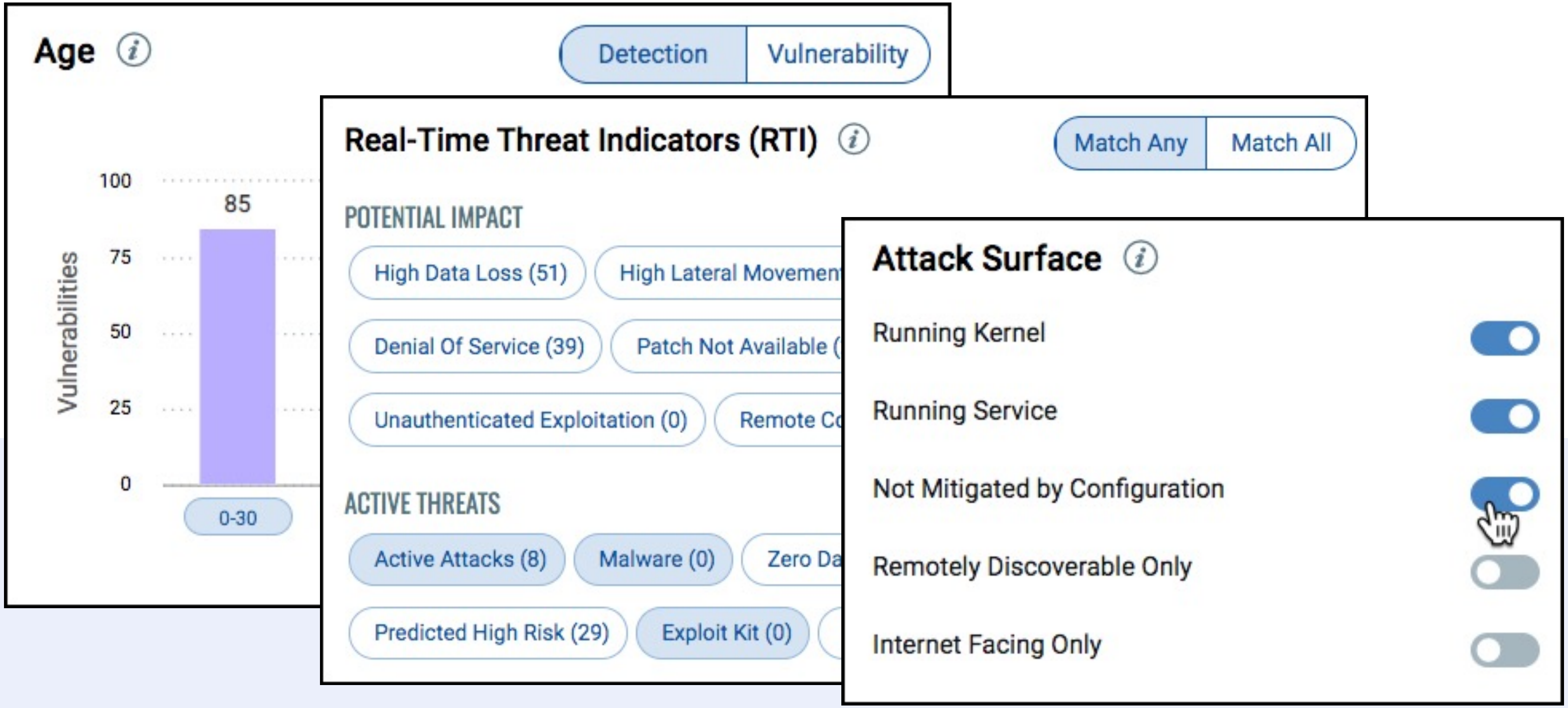


Start Adding Asset Tags...

□ Database Server
□ Cloud Agent
□ Malware Domain...
□ SJC
□ VMDR Lab
□ File Transfer
□ Internet Facing...
□ Web Server
□ Business Units
□ EOL/EOS
□ Security Tools
□ Compiler

- Design and build Asset Tags that help to distinguish the “context” of your assets.
- Leverage tags that use the “Asset Inventory” rule engine, along with 1) hardware, 2) software, and 3) OS categories.

Priority Options



Real-Time Threat Indicators (RTI)

POTENTIAL IMPACT

High Data Loss (51) | High Lateral Movement | Denial Of Service (39) | Patch Not Available (| Unauthenticated Exploitation (0) | Remote Co

ACTIVE THREATS

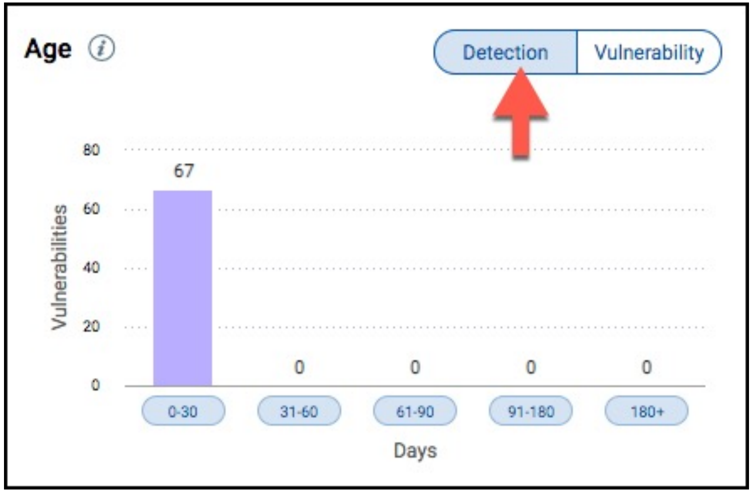
Active Attacks (8) | Malware (0) | Zero Da | Predicted High Risk (29) | Exploit Kit (0)

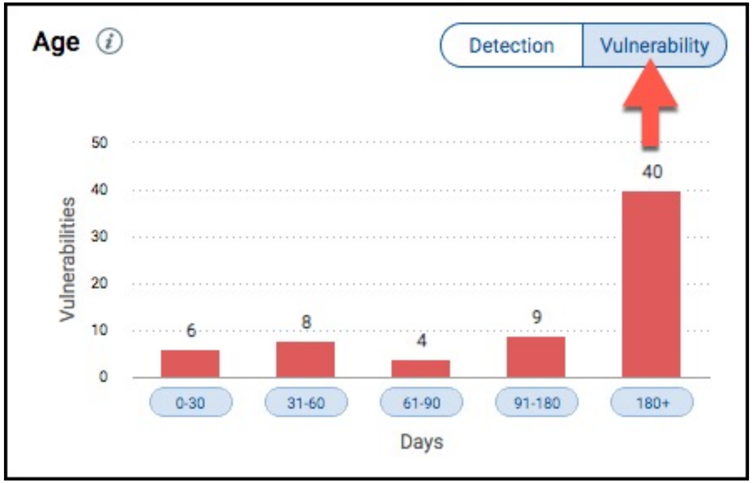
Attack Surface

- Running Kernel ●
- Running Service ●
- Not Mitigated by Configuration ●
- Remotely Discoverable Only ○
- Internet Facing Only ○

Prioritize discovered vulnerabilities by Age, RTIs, and Attack Surface.

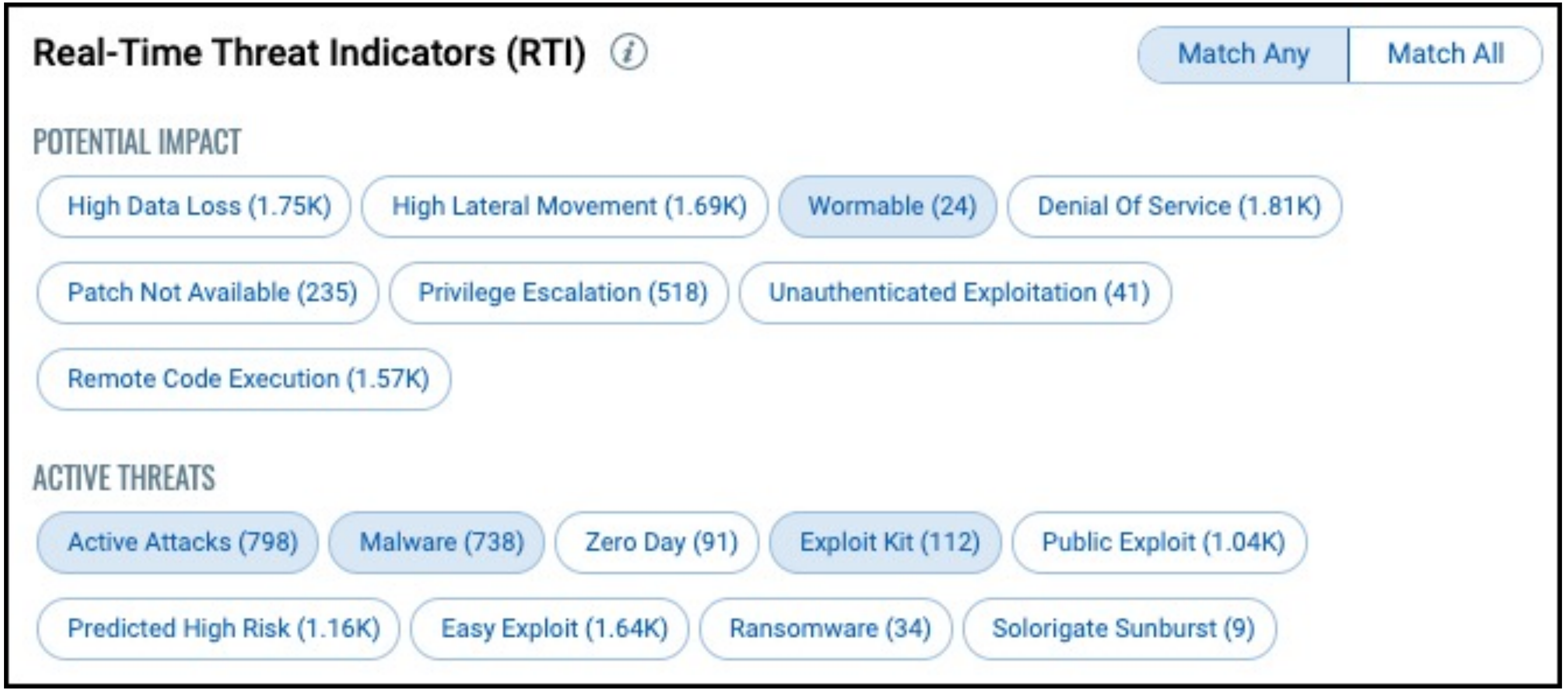
Age





- **Detection Age** – reflects the number of days since you first detected the vulnerability (e.g., by Qualys scanner or Cloud Agent).
- **Vulnerability Age** – (i.e., real age) reflects the number days since Qualys published the vulnerability to our KnowledgeBase.

Real-Time Threat Indicators (RTI)



Real-Time Threat Indicators (RTI) ⓘ

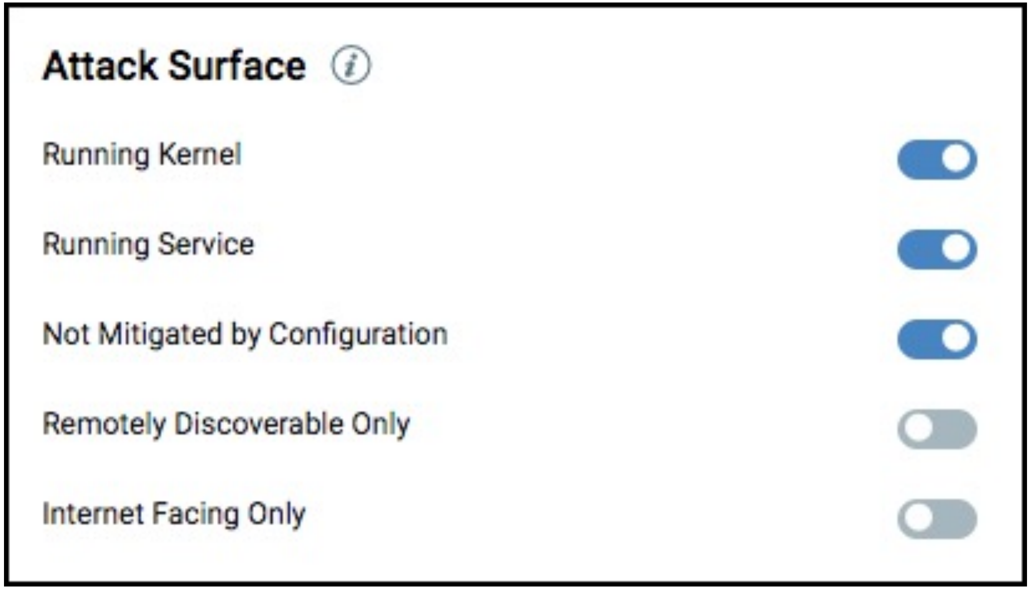
POTENTIAL IMPACT

High Data Loss (1.75K)
High Lateral Movement (1.69K)
Wormable (24)
Denial Of Service (1.81K)
Patch Not Available (235)
Privilege Escalation (518)
Unauthenticated Exploitation (41)
Remote Code Execution (1.57K)

ACTIVE THREATS

- Provided by VMDR Threat Feed.

Attack Surface

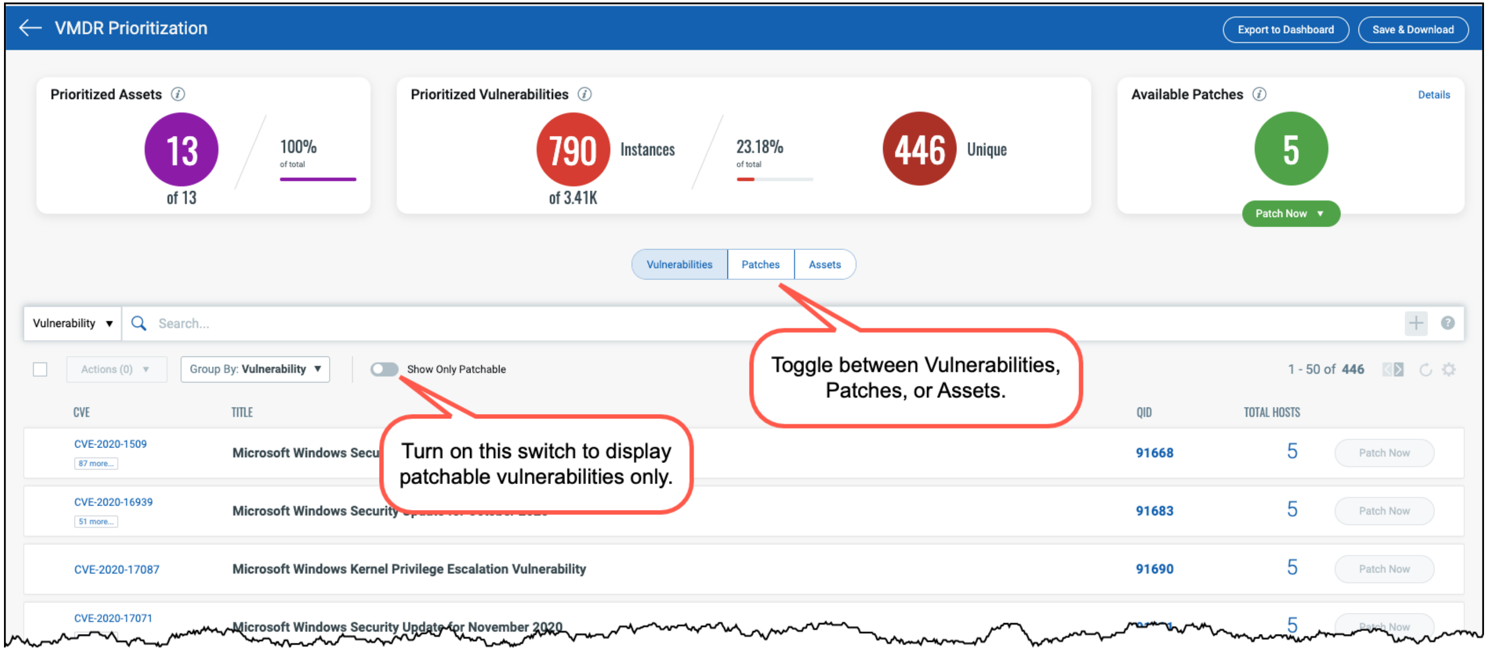


Attack Surface ⓘ

- Running Kernel ☑
- Running Service ☑
- Not Mitigated by Configuration ☑
- Remotely Discoverable Only ☐
- Internet Facing Only ☐

Continue to define asset context with “Attack Surface” options.

Deploy Priority Patches



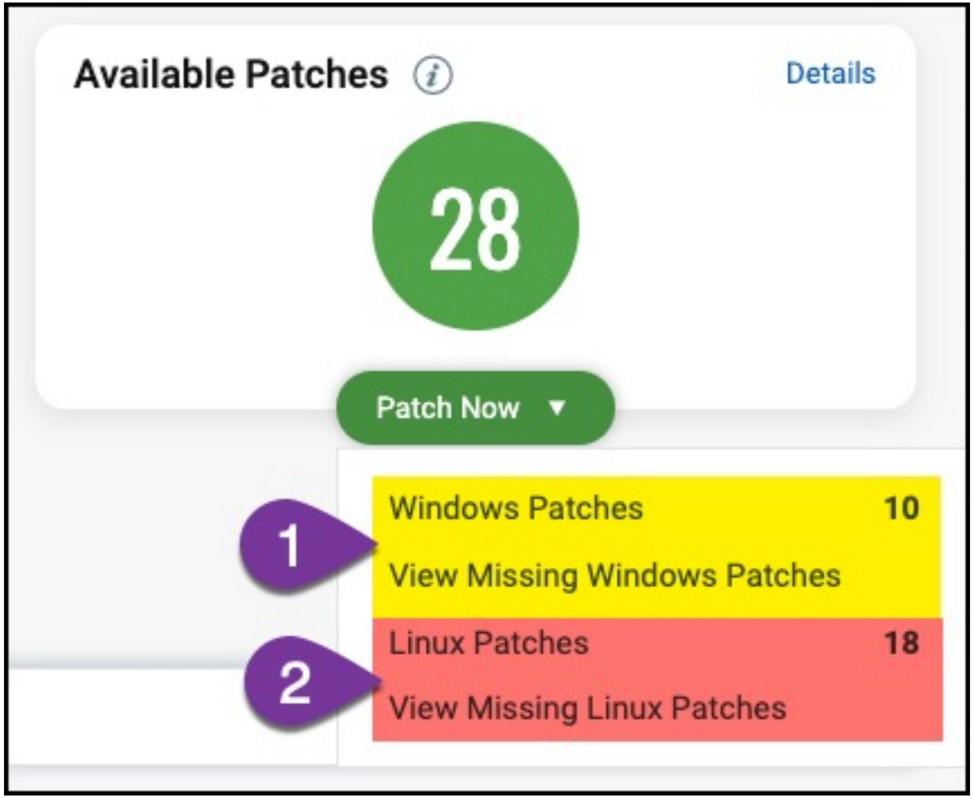
CVE	TITLE	QID	TOTAL HOSTS	
CVE-2020-1509 87 more...	Microsoft Windows Secu	91668	5	Patch Now
CVE-2020-16939 51 more...	Microsoft Windows Security	91683	5	Patch Now
CVE-2020-17087	Microsoft Windows Kernel Privilege Escalation Vulnerability	91690	5	Patch Now
CVE-2020-17071	Microsoft Windows Security Update for November 2020		5	Patch Now

Toggle between Vulnerabilities, Patches, or Assets.

Turn on this switch to display patchable vulnerabilities only.

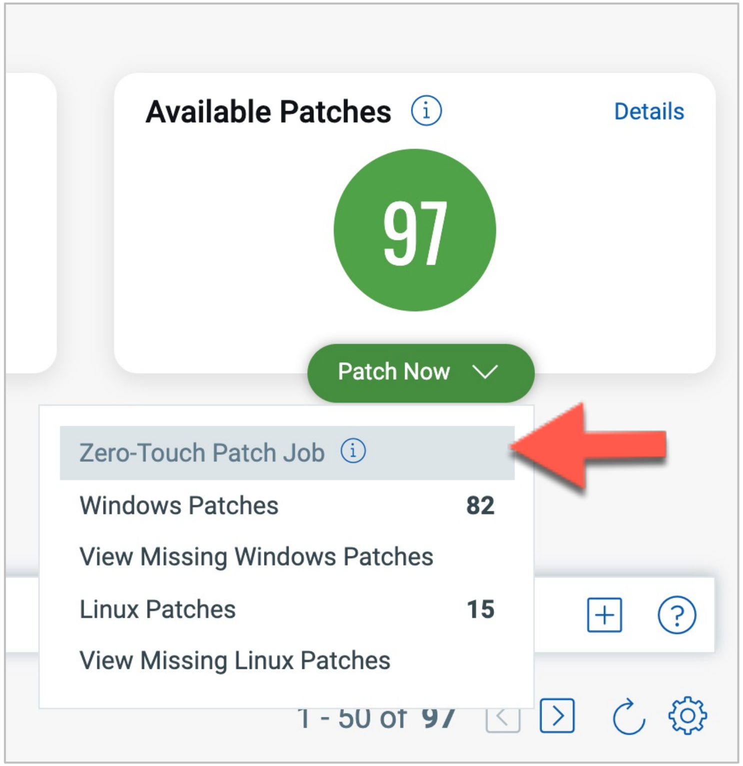
Patchable assets have Cloud Agent installed and Patch Management activated.

Windows & Linux Patches



1. Available patches provided for Windows hosts.
2. Available patches provide for Linux hosts.

Zero-Touch Patch Job



- Select the “Zero-Touch Patch Job” option from the VMDR Prioritization Report.
- Patches are not selected individually, but instead are targeted using a query.
- Schedule patch jobs to recur daily, weekly, or monthly.
- Specific patching use-cases are ideal for ”Zero-Touch” patching.

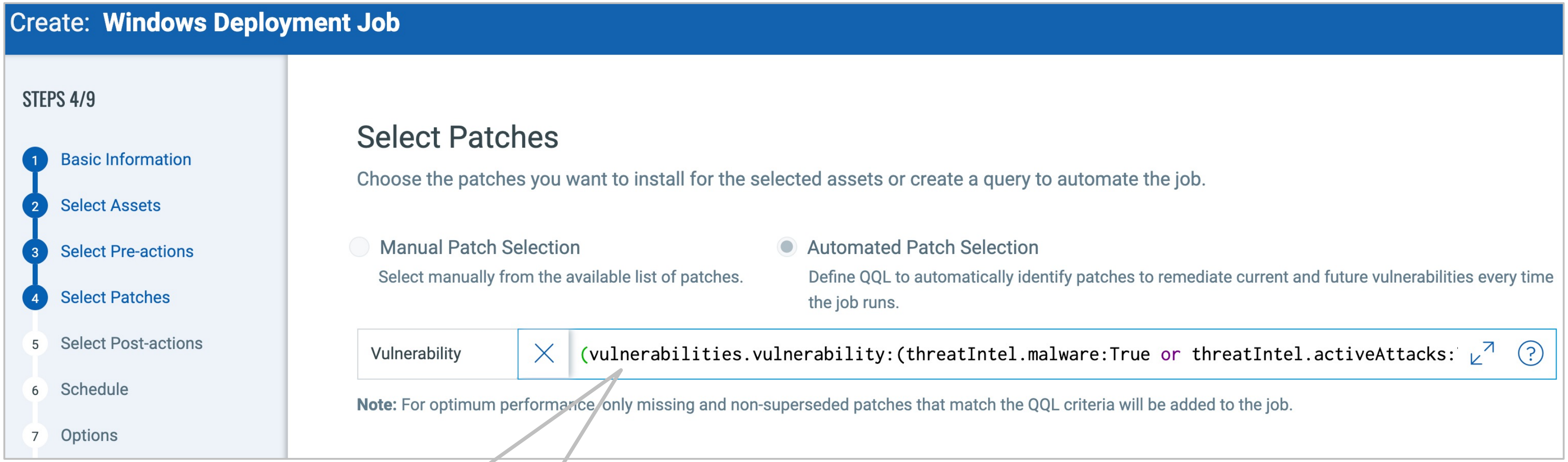
Lab 13 : Zero-Touch Patch Job

Please consult page 50 in the lab tutorial supplement for details.

PLAY Tutorials begins on page 50.

5 min.

Automated Patch Selection



Create: **Windows Deployment Job**

STEPS 4/9

1 Basic Information
2 Select Assets
3 Select Pre-actions
4 Select Patches
5 Select Post-actions
6 Schedule
7 Options

Select Patches

Choose the patches you want to install for the selected assets or create a query to automate the job.

○ Manual Patch Selection
Select manually from the available list of patches.

● Automated Patch Selection
Define QQL to automatically identify patches to remediate current and future vulnerabilities every time the job runs.

Vulnerability

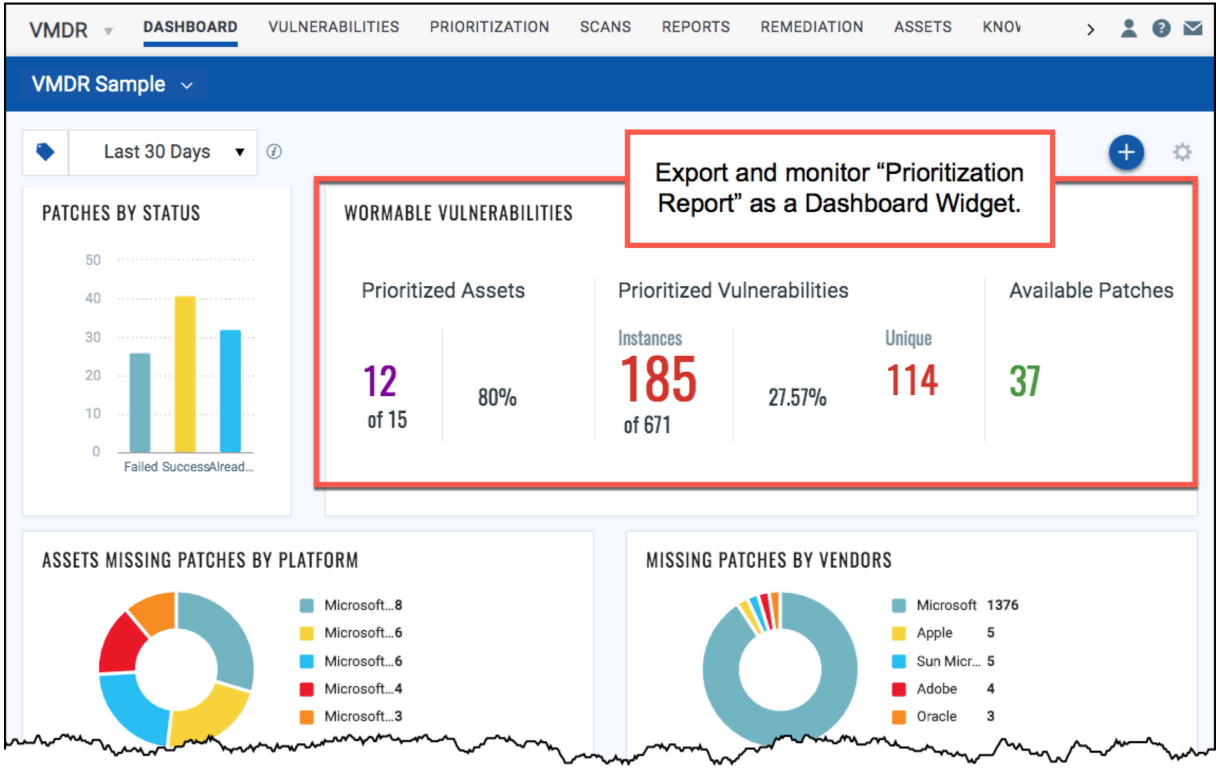
```
(vulnerabilities.vulnerability:(threatIntel.malware:True or threatIntel.activeAttacks:
```

Note: For optimum performance, only missing and non-superseded patches that match the QQL criteria will be added to the job.

Patches that meet the query condition are added to the deployment job, automatically.

- The query is generated from the options (Age, RTIs, and Attack Surface) selected in the Prioritization Report.

Export to Dashboard



Export and monitor "Prioritization Report" as a Dashboard Widget.

Results will be continuously updated within the Dashboard Widget.

Patch Management

Patch Management Overview

- Automatically correlates discovered vulnerabilities with their required patches

- Leverage existing Qualys Cloud Agents to deploy and uninstall patches

- Provides OS and Application patches, including patches from third-party software vendors (e.g., Adobe, Java, Google, Mozilla, Microsoft, etc...)

Patch Management Overview (cont.)

- Available for Windows, CentOS 6/7, and RHEL 6/7/8
- Provides patching just about anywhere an Internet connection is available (e.g., airports, coffee shops, remote offices, etc...)
- Qualys Agents determine which patches are missing or required and can identify superseded patches
- Build patch jobs that target specific vulnerabilities, severity levels, and known threats

Patch Sources

OS and Application Patches come from:

- Vendor Global CDNs (e.g., Oracle, Adobe, Microsoft, Apache, Google, etc...)
- YUM repositories (Linux)
- Local repository (i.e., Qualys Gateway Server)
  - Patch downloads requested by one agent, are cached on QGS and made available “locally” for other agents that need the same patch.
  - QGS also provides a cache for manifests and agent binaries

Qualys PM Workflow

CA 1. Install Cloud Agent on target host.

CA 2. Assign target agent host to a CA Configuration Profile that has PM configuration enabled.

CA 3. Activate PM module on target agent host.

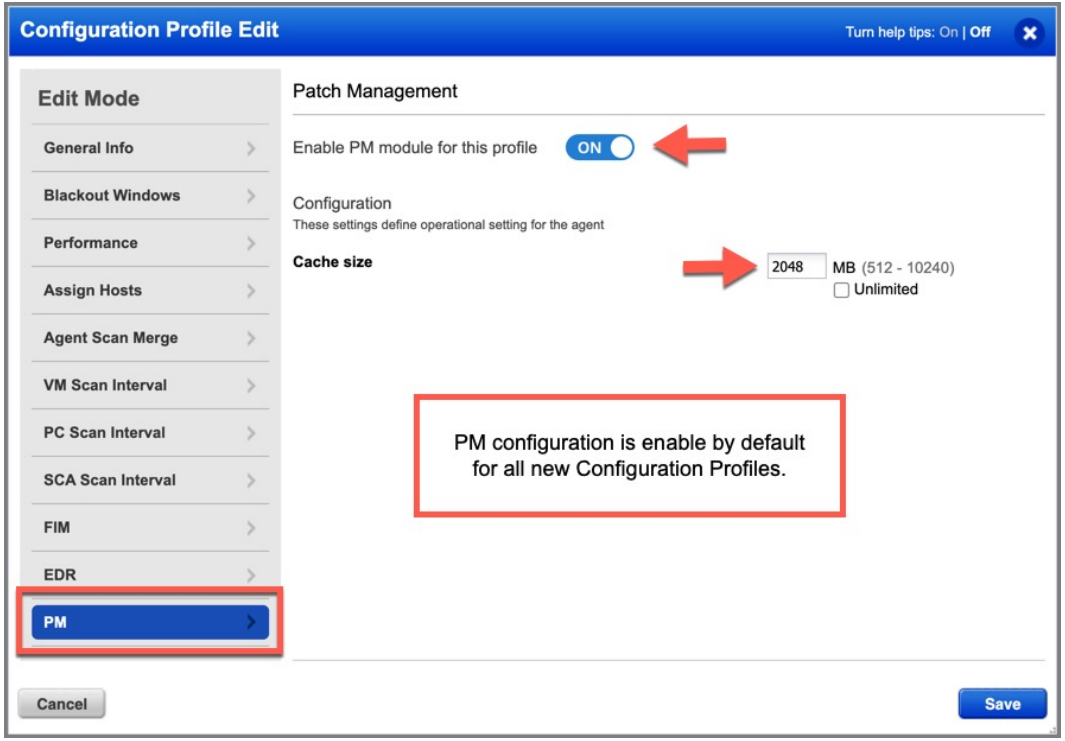
PM 4. Assign target agent host to an enabled Assessment Profile.

PM 5. Allocate patching licenses.

PM 6. Create Patch Jobs.

Configuration Profile

CA



Patch Management

Enable PM module for this profile ON

Configuration

These settings define operational setting for the agent

Cache size 2048 MB (512 - 10240)

□ Unlimited

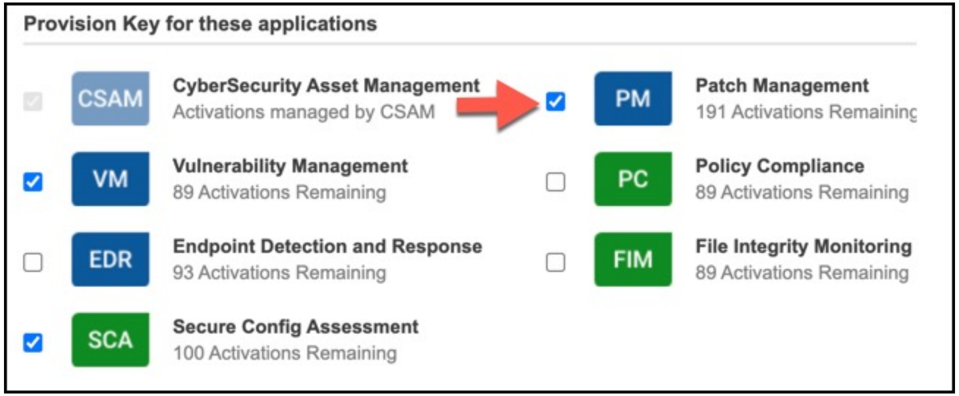
PM configuration is enable by default for all new Configuration Profiles.

- Presently, PM has one agent configuration setting.
- Set "Cache size" to at least 2048 MB, to accommodate Windows Updates.

Qualys.

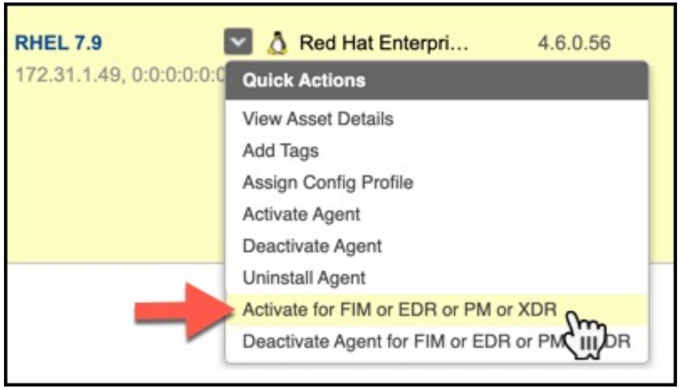
Activate PM Module for Target Host

- Select the PM module in the Agent Activation Key, before and after agent deployment.



Provision Key for these applications

☑	CSAM	**CyberSecurity Asset Management** Activations managed by CSAM	☑	PM	**Patch Management** 191 Activations Remaining
☑	VM	**Vulnerability Management** 89 Activations Remaining	□	PC	**Policy Compliance** 89 Activations Remaining
□	EDR	**Endpoint Detection and Response** 93 Activations Remaining	□	FIM	**File Integrity Monitoring** 89 Activations Remaining
☑	SCA	**Secure Config Assessment** 100 Activations Remaining			



RHEL 7.9 Red Hat Enterpri... 4.6.0.56

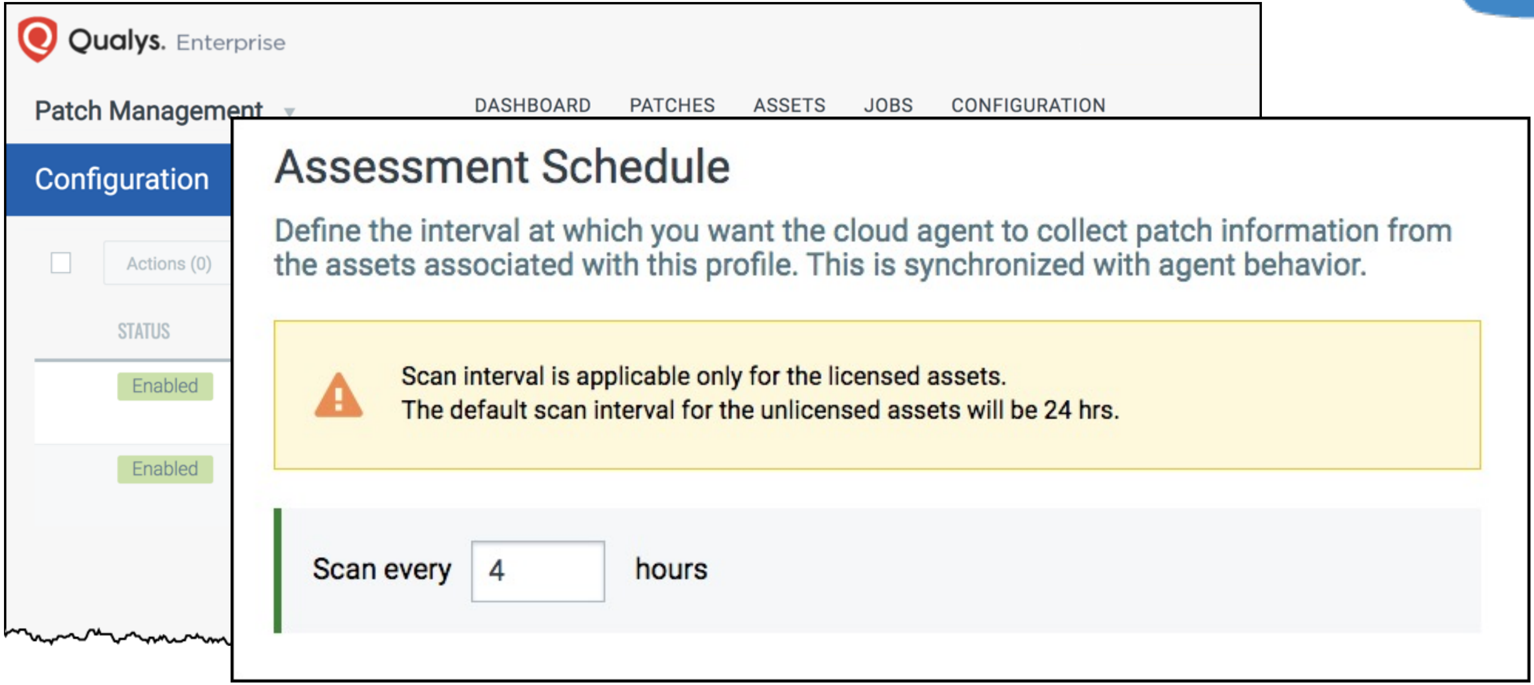
172.31.1.49, 0:0:0:0:0:0

Quick Actions

- View Asset Details
- Add Tags
- Assign Config Profile
- Activate Agent
- Deactivate Agent
- Uninstall Agent
- Activate for FIM or EDR or PM or XDR
- Deactivate Agent for FIM or EDR or PM or XDR

- Use the “Quick Actions” menu to activate PM for any agent host or use the Qualys Cloud Agent API.

Assessment Profile



Assessment Schedule

Define the interval at which you want the cloud agent to collect patch information from the assets associated with this profile. This is synchronized with agent behavior.

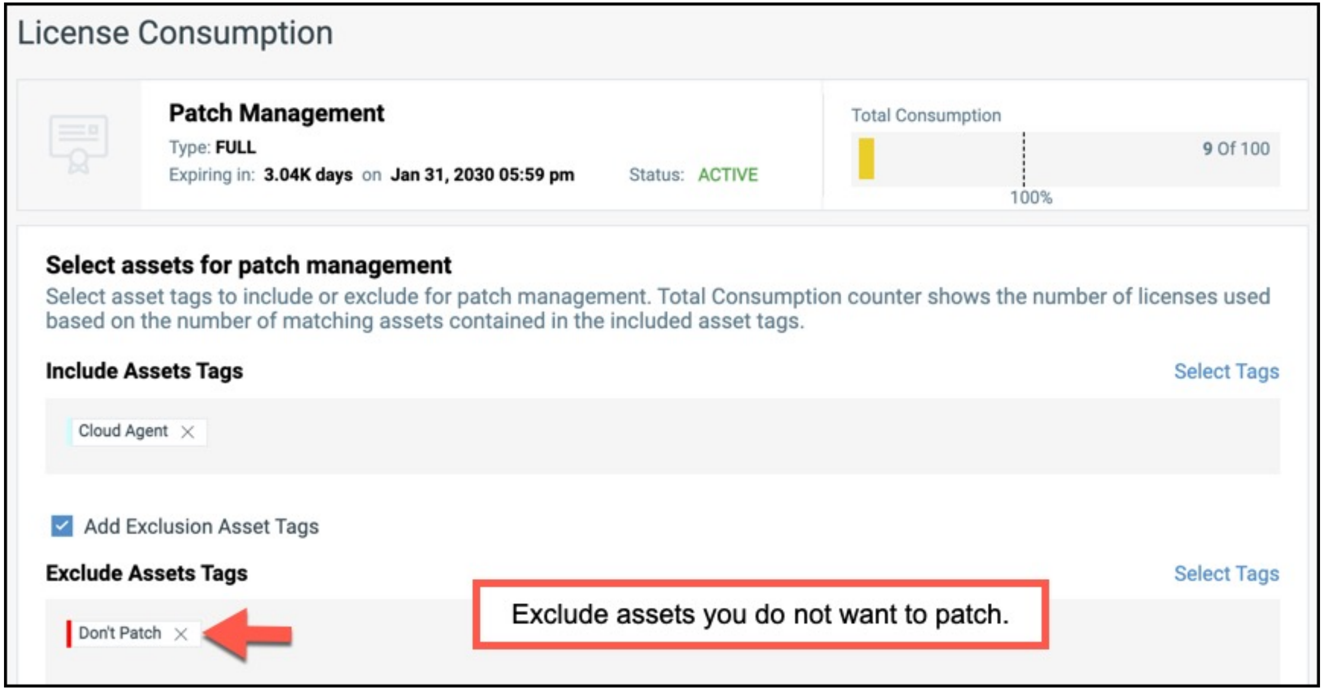
Scan interval is applicable only for the licensed assets.
The default scan interval for the unlicensed assets will be 24 hrs.

Scan every 4 hours

- Specifies frequency of patch assessment scans.
- System Profile will be used by default.

License Consumption

PM



License Consumption

Patch Management

Type: **FULL**

Expiring in: **3.04K days** on **Jan 31, 2030 05:59 pm** Status: ACTIVE

Total Consumption

Select assets for patch management

Select asset tags to include or exclude for patch management. Total Consumption counter shows the number of licenses used based on the number of matching assets contained in the included asset tags.

Include Assets Tags Select Tags

Cloud Agent ×

☑ Add Exclusion Asset Tags

Exclude Assets Tags Select Tags

Don't Patch ×

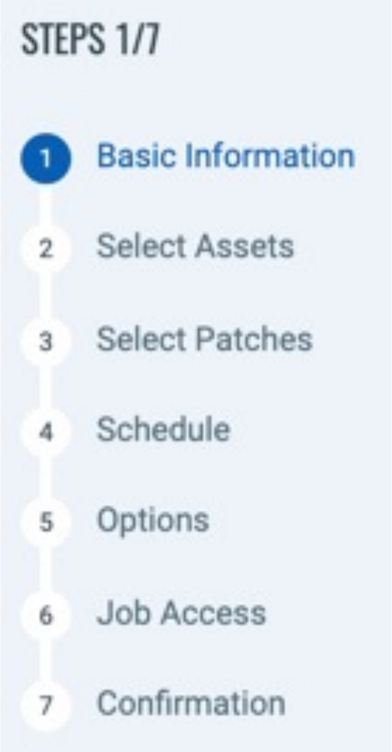
Exclude assets you do not want to patch.

- Use Asset Tags to specify hosts for patching and to exclude others.
- Only agent host assets will consume a patch license.

Qualys.

Patch Deployment Job

Deployment Job Wizard



STEPS 1/7

1 Basic Information

2 Select Assets

3 Select Patches

4 Schedule

5 Options

6 Job Access

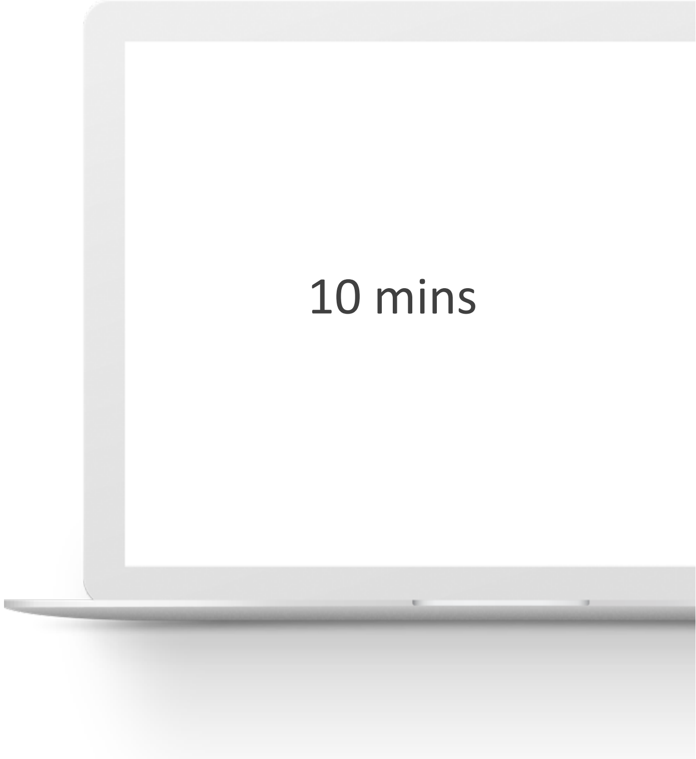
7 Confirmation

- Build patch jobs step-by-step.
- Select assets and patches.
- Configure scheduling option or run on-demand.
- Configure communication and reboot options.
- Assign access to a job.

Lab 14 : Patch Deployment

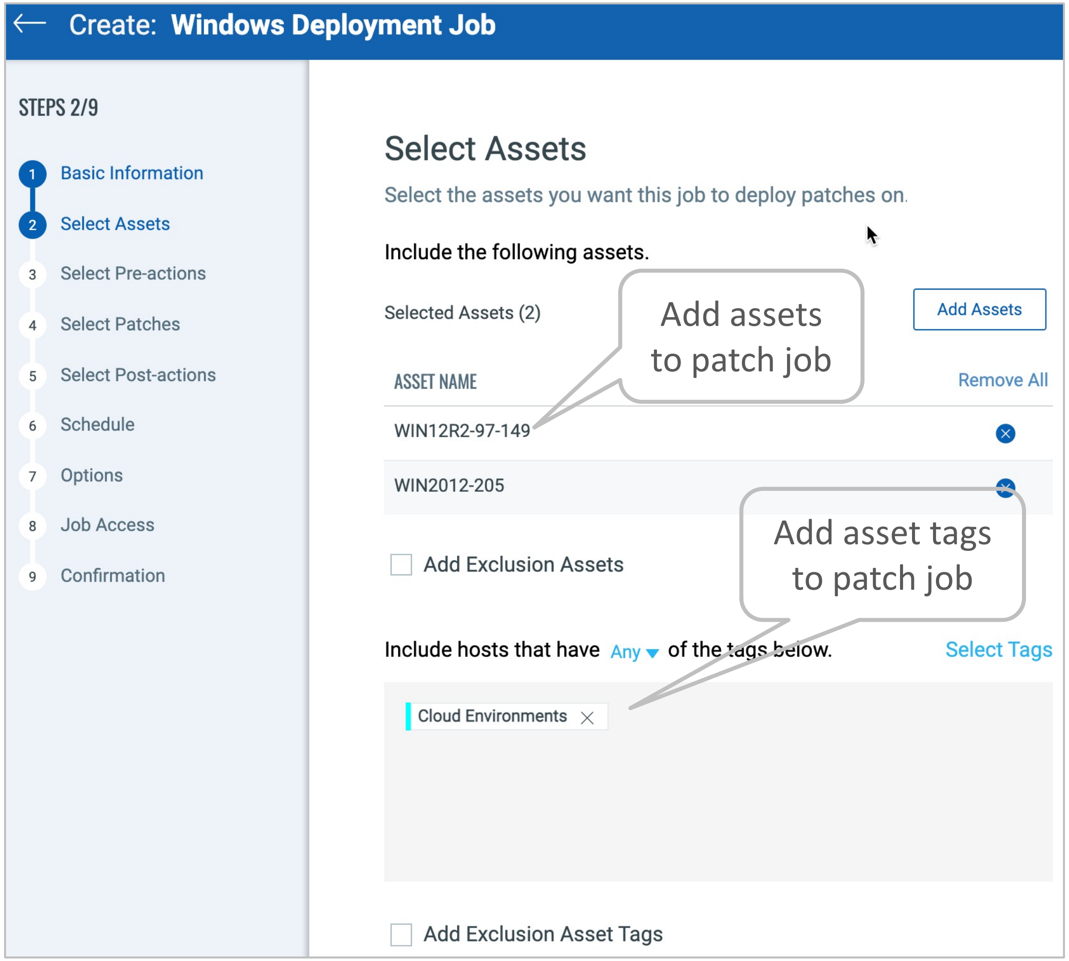
Please consult pages 52 to 57 in the lab tutorial supplement for details.

PLAY Tutorial begins on page 52.



10 mins

Select Assets



← Create: **Windows Deployment Job**

STEPS 2/9

1. Basic Information
2. Select Assets
3. Select Pre-actions
4. Select Patches
5. Select Post-actions
6. Schedule
7. Options
8. Job Access
9. Confirmation

Select Assets

Select the assets you want this job to deploy patches on.

Include the following assets.

Selected Assets (2)

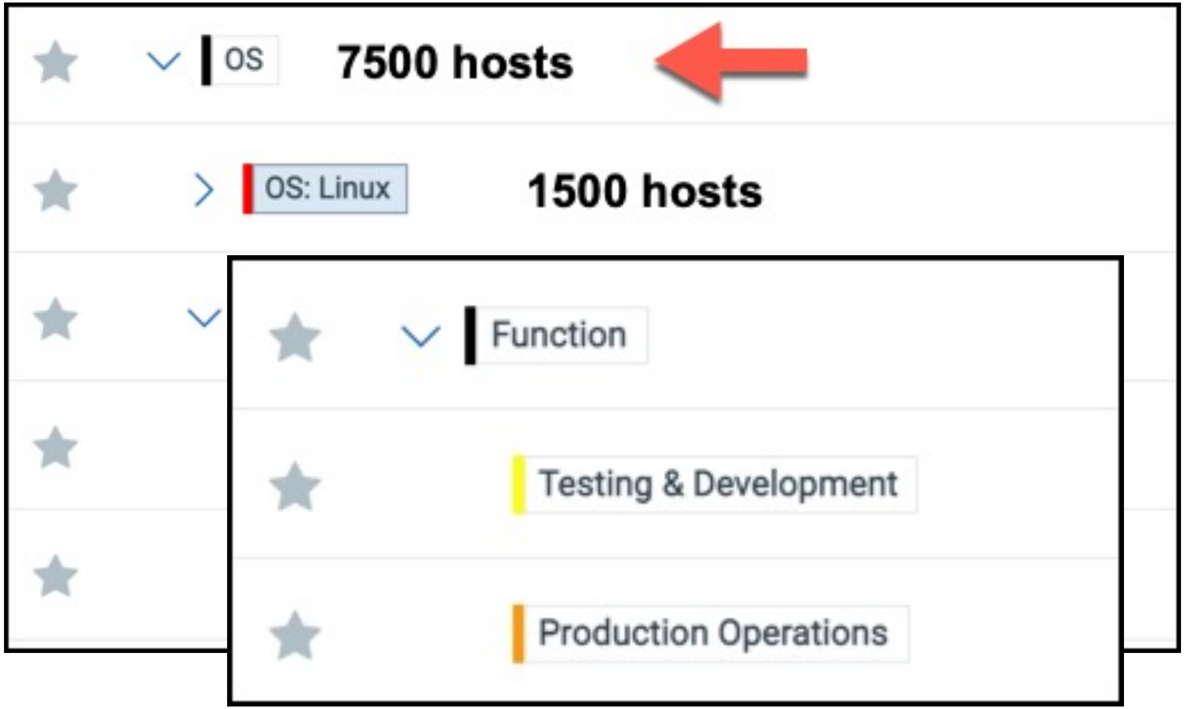
ASSET NAME
WIN12R2-97-149
WIN2012-205

□ Add Exclusion Assets

Include hosts that have Any of the tags below.

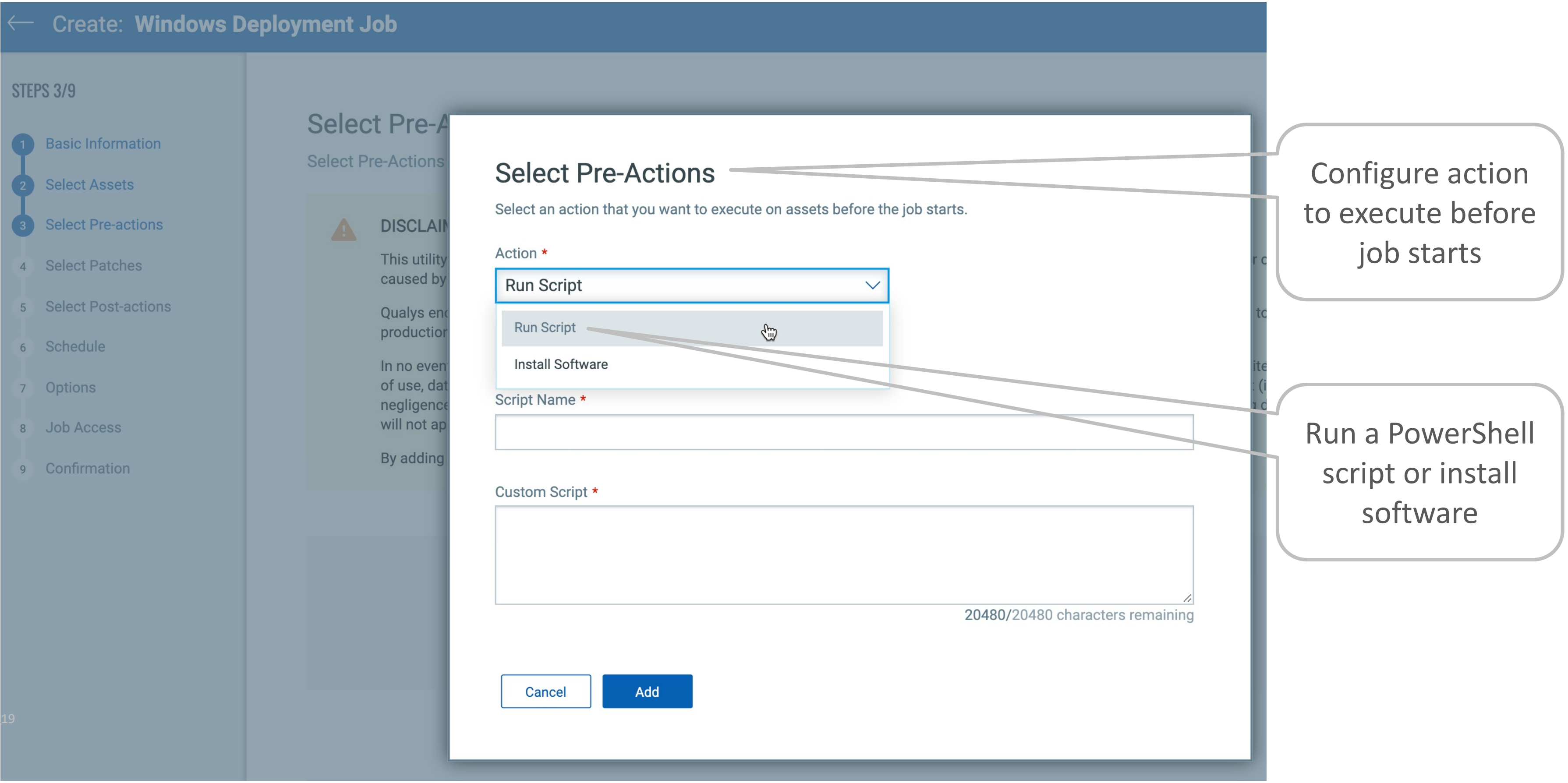
□ Add Exclusion Asset Tags

Asset Tag Tips



- Design Asset Tag hierarchies with nested structures.
- Selecting a “parent” tag as a patching target, includes its “child” tags automatically.
- Use tags to distinguish between production and testing assets.

Pre and Post Actions



Select Pre-Actions

Select an action that you want to execute on assets before the job starts.

Action *: Run Script

Script Name *

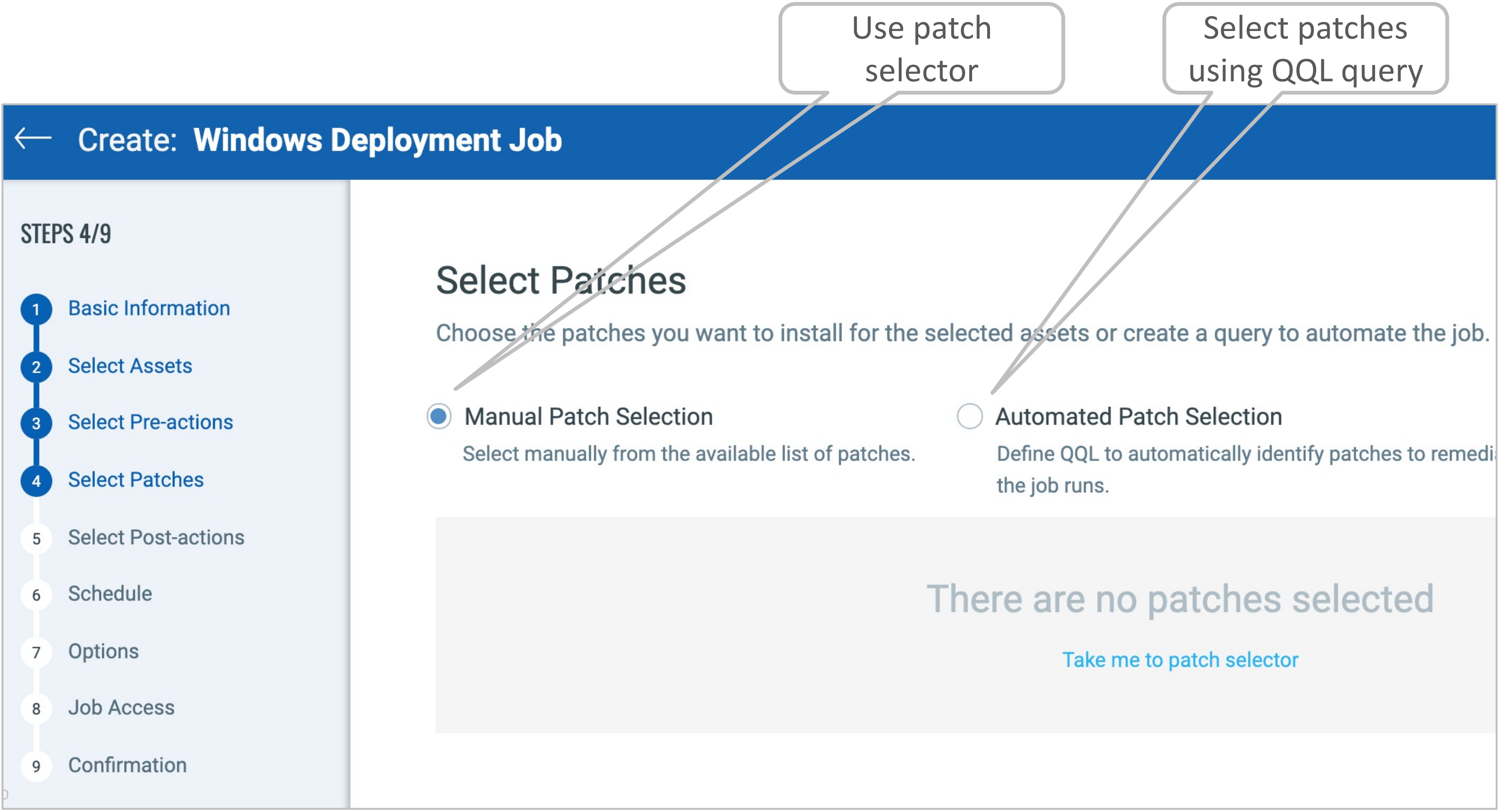
Custom Script *

20480/20480 characters remaining

Configure action to execute before job starts

Run a PowerShell script or install software

Select Patches



Use patch selector

Select patches using QQL query

← Create: **Windows Deployment Job**

STEPS 4/9

1 Basic Information
2 Select Assets
3 Select Pre-actions
4 Select Patches
5 Select Post-actions
6 Schedule
7 Options
8 Job Access
9 Confirmation

Select Patches

Choose the patches you want to install for the selected assets or create a query to automate the job.

● Manual Patch Selection
Select manually from the available list of patches.

○ Automated Patch Selection
Define QQL to automatically identify patches to remedi
the job runs.

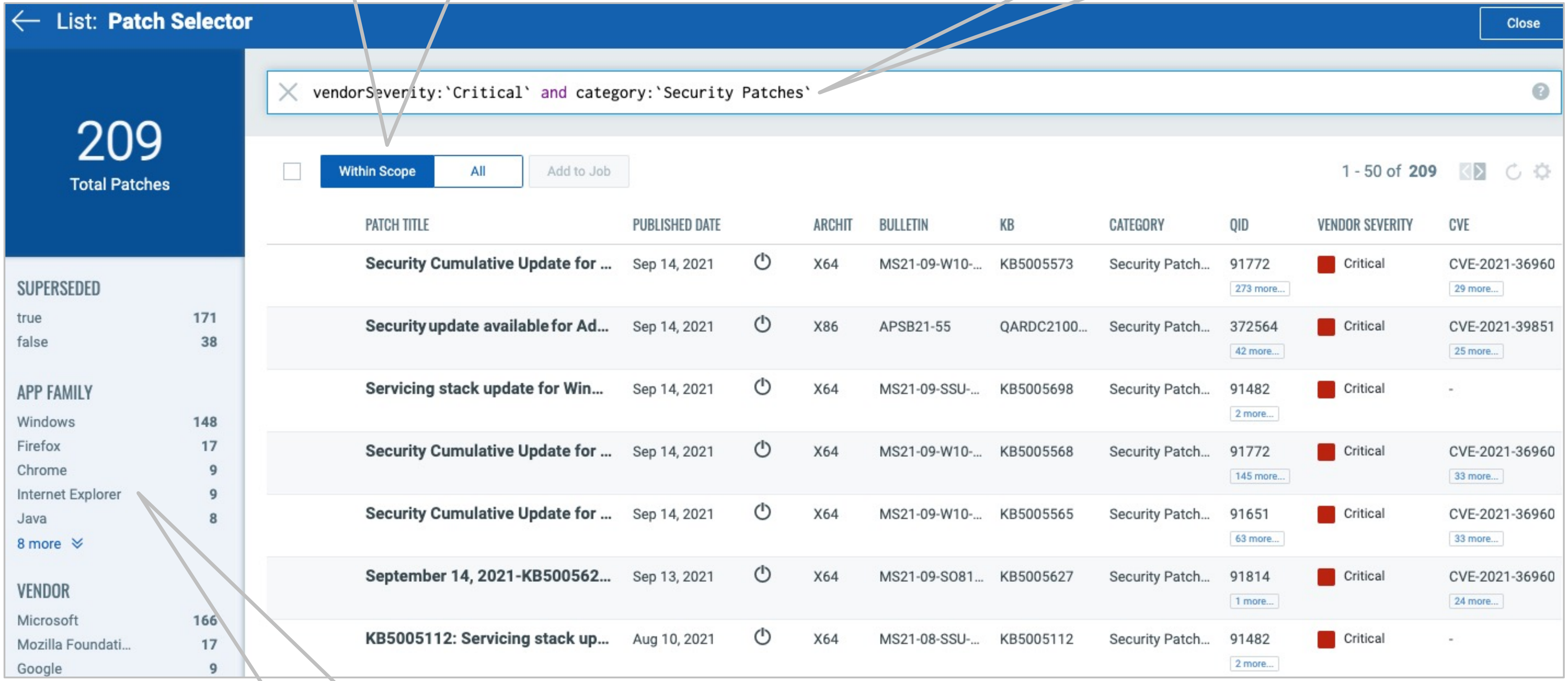
There are no patches selected

Take me to patch selector

Manual Patch Selection

View patches within scope of selected assets

Use queries to narrow selections



← List: **Patch Selector**

Close

```
vendorSeverity:`Critical` and category:`Security Patches`
```

209
Total Patches

SUPERSEDED

true	171
false	38

APP FAMILY

Windows	148
Firefox	17
Chrome	9
Internet Explorer	9
Java	8

8 more

VENDOR

Microsoft	166
Mozilla Foundati...	17
Google	9

□ Within Scope | All | Add to Job

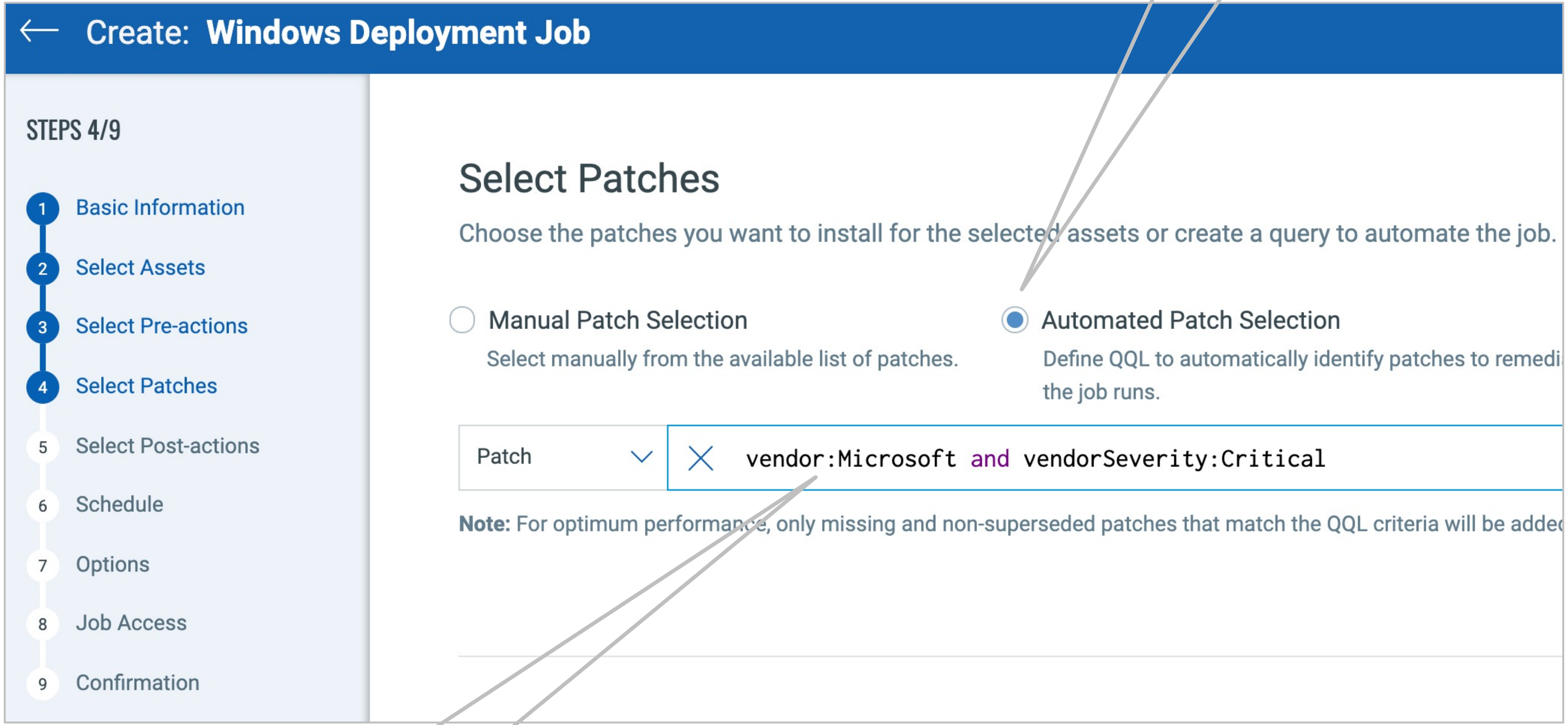
1 - 50 of **209**

PATCH TITLE	PUBLISHED DATE		ARCHIT	BULLETIN	KB	CATEGORY	QID	VENDOR SEVERITY	CVE
Security Cumulative Update for ...	Sep 14, 2021	⏻	X64	MS21-09-W10-...	KB5005573	Security Patch...	91772 273 more...	🟥 Critical	CVE-2021-36960 29 more...
Security update available for Ad...	Sep 14, 2021	⏻	X86	APSB21-55	QARDC2100...	Security Patch...	372564 42 more...	🟥 Critical	CVE-2021-39851 25 more...
Servicing stack update for Win...	Sep 14, 2021	⏻	X64	MS21-09-SSU-...	KB5005698	Security Patch...	91482 2 more...	🟥 Critical	-
Security Cumulative Update for ...	Sep 14, 2021	⏻	X64	MS21-09-W10-...	KB5005568	Security Patch...	91772 145 more...	🟥 Critical	CVE-2021-36960 33 more...
Security Cumulative Update for ...	Sep 14, 2021	⏻	X64	MS21-09-W10-...	KB5005565	Security Patch...	91651 63 more...	🟥 Critical	CVE-2021-36960 33 more...
September 14, 2021-KB500562...	Sep 13, 2021	⏻	X64	MS21-09-SO81...	KB5005627	Security Patch...	91814 1 more...	🟥 Critical	CVE-2021-36960 24 more...
KB5005112: Servicing stack up...	Aug 10, 2021	⏻	X64	MS21-08-SSU-...	KB5005112	Security Patch...	91482 2 more...	🟥 Critical	-

Use filters to narrow selections

Automated Patch Selection

Select patches using QQL query



← Create: **Windows Deployment Job**

STEPS 4/9

1. Basic Information
2. Select Assets
3. Select Pre-actions
4. Select Patches
5. Select Post-actions
6. Schedule
7. Options
8. Job Access
9. Confirmation

Select Patches

Choose the patches you want to install for the selected assets or create a query to automate the job.

○ Manual Patch Selection
Select manually from the available list of patches.

● Automated Patch Selection
Define QQL to automatically identify patches to remedi
the job runs.

Patch ⌵ ✕

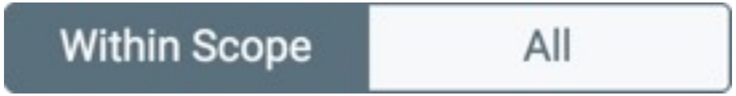
```
vendor:Microsoft and vendorSeverity:Critical
```

Note: For optimum performance, only missing and non-superseded patches that match the QQL criteria will be addec

Use a query to select patches

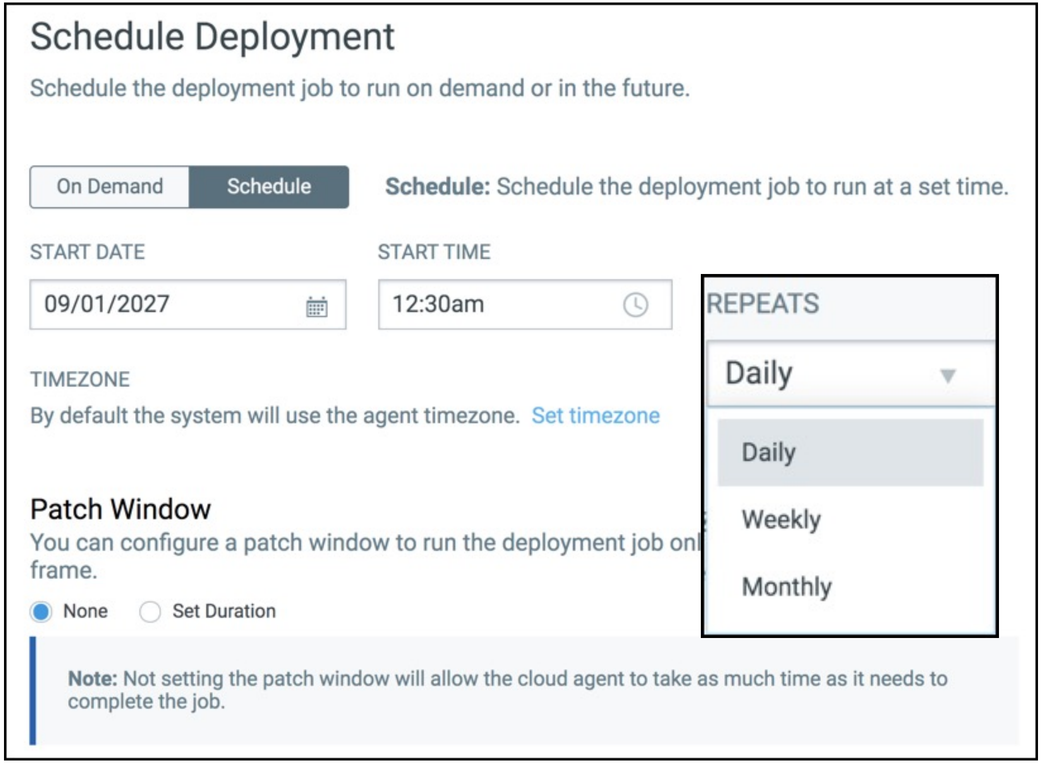
Qualys.

“Within Scope” Patch



“Within Scope” only includes patches needed by your targeted host assets.

Schedule Deployment



Schedule Deployment

Schedule the deployment job to run on demand or in the future.

Schedule: Schedule the deployment job to run at a set time.

START DATE: 09/01/2027

START TIME: 12:30am

REPEATS: Daily

TIMEZONE

By default the system will use the agent timezone. Set timezone

Patch Window

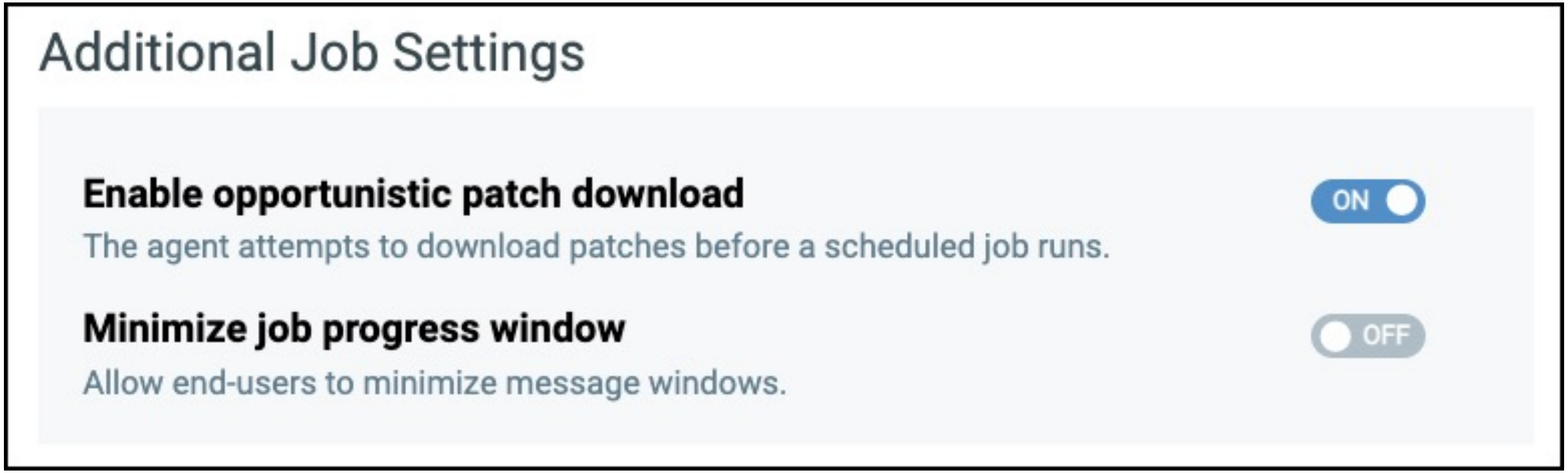
You can configure a patch window to run the deployment job onl
frame.

● None ○ Set Duration

Note: Not setting the patch window will allow the cloud agent to take as much time as it needs to complete the job.

Run jobs ”on demand” or schedule them to run at regular frequencies.

Opportunistic Patch Download



Additional Job Settings

Enable opportunistic patch download

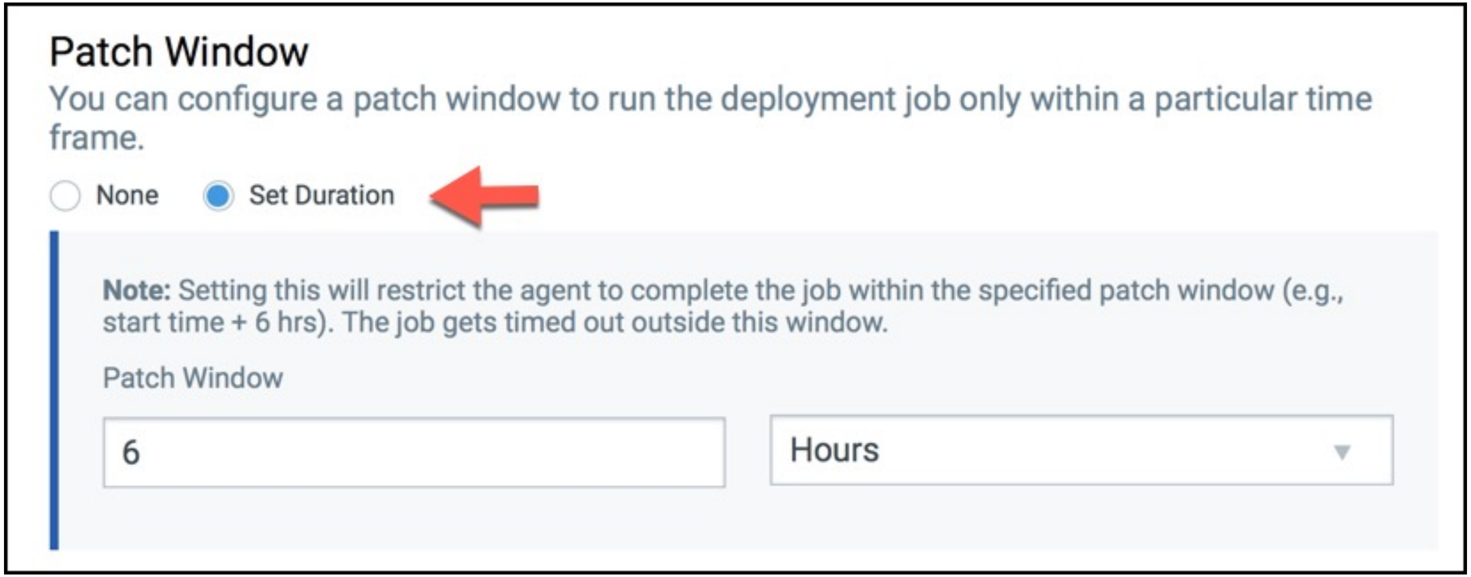
The agent attempts to download patches before a scheduled job runs.

Minimize job progress window

Allow end-users to minimize message windows.

You can “Enable opportunistic patch download,” to allow agents to download required patches prior to the start of a scheduled job.

Patch Window



Patch Window

You can configure a patch window to run the deployment job only within a particular time frame.

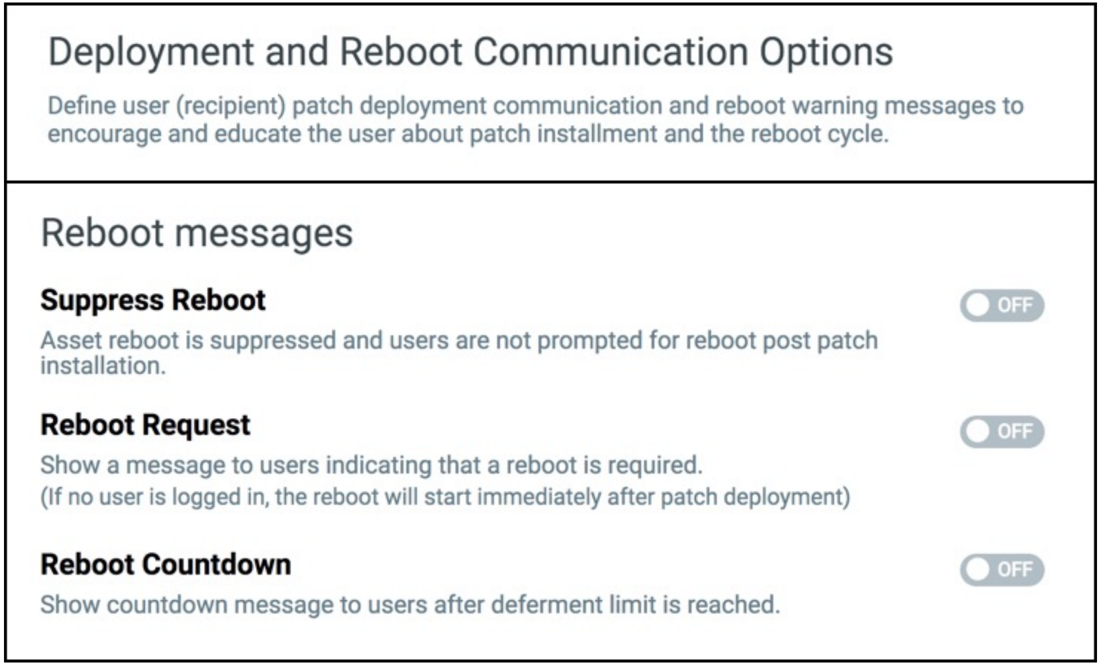
○ None ● Set Duration

Note: Setting this will restrict the agent to complete the job within the specified patch window (e.g., start time + 6 hrs). The job gets timed out outside this window.

Patch Window: 6 Hours

- A host will display the “Timed out” status, if the patch installation does not start within a specified patch window.
- Select the “None” option to give agents an unlimited amount of time.

Windows Communication Options



Deployment and Reboot Communication Options

Define user (recipient) patch deployment communication and reboot warning messages to encourage and educate the user about patch installment and the reboot cycle.

Reboot messages

Suppress Reboot OFF

Asset reboot is suppressed and users are not prompted for reboot post patch installation.

Reboot Request OFF

Show a message to users indicating that a reboot is required.
(If no user is logged in, the reboot will start immediately after patch deployment)

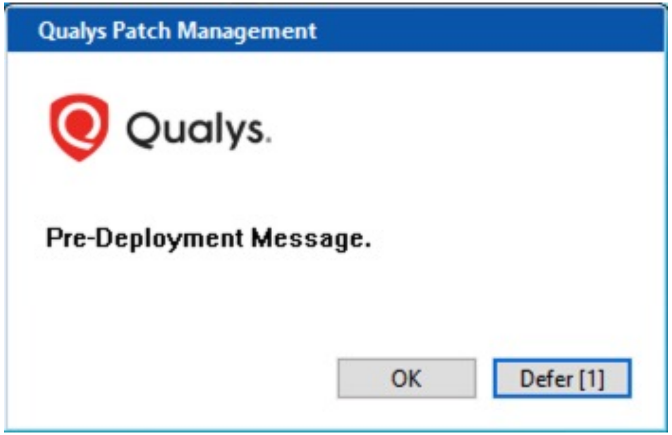
Reboot Countdown OFF

Show countdown message to users after deferment limit is reached.

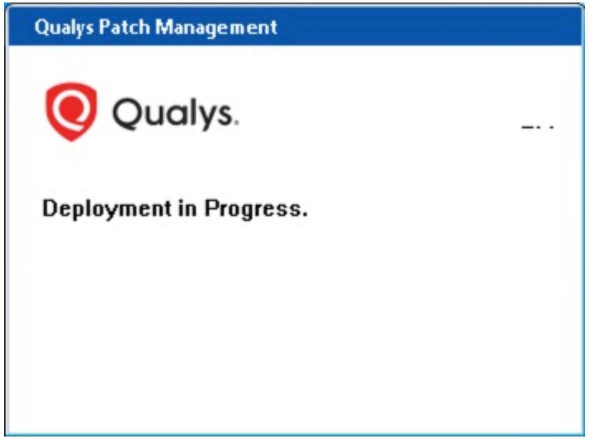
Choose the type of “Deployment and Reboot Communication Options” for each Deployment Job.

Host “Pop-Up” Messages

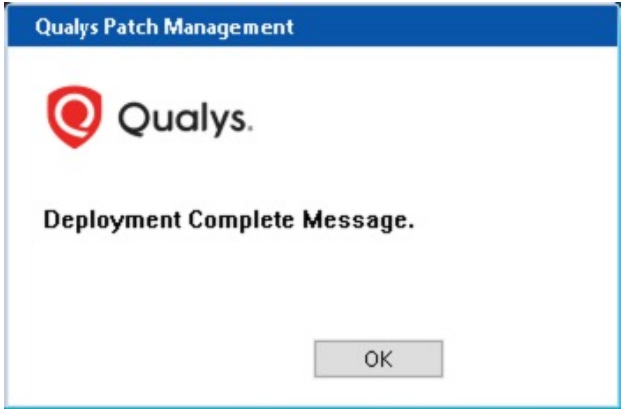
“Pre-Deployment and “Reboot Request messages can be configured with deferment options.



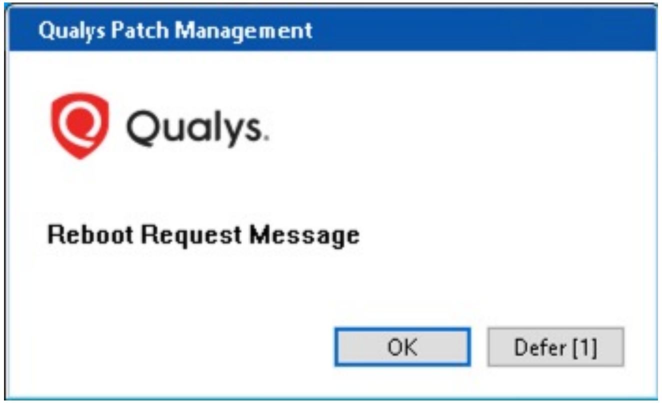
Pre-Deployment Message.



Deployment in Progress.

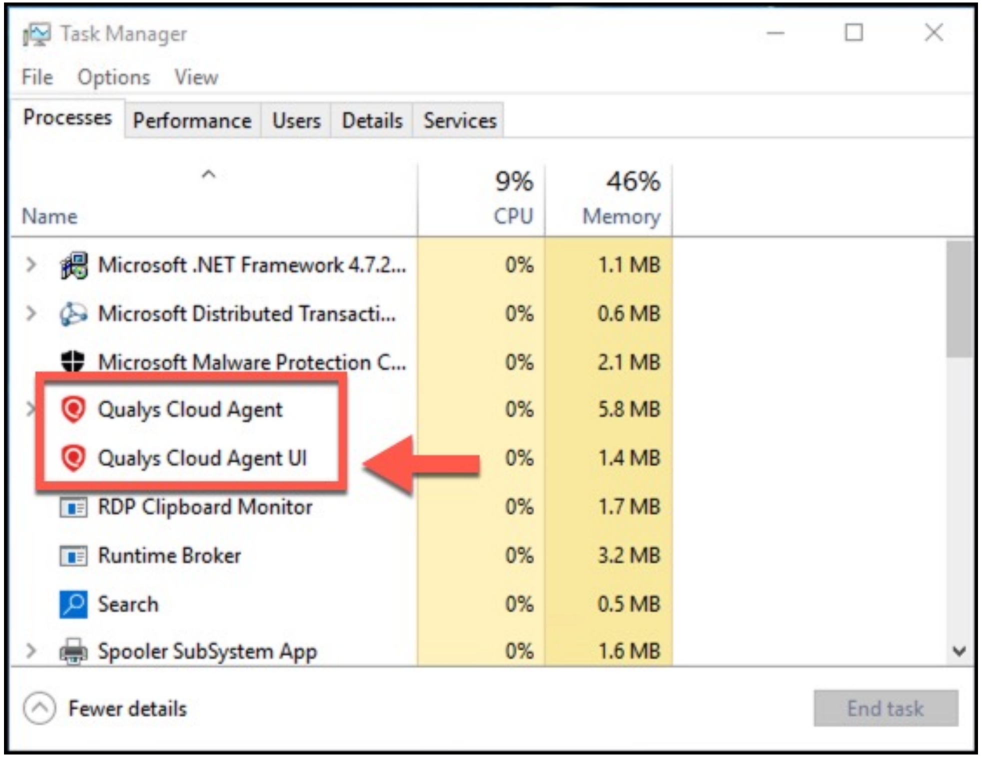


Deployment Complete Message.



Reboot Request Message

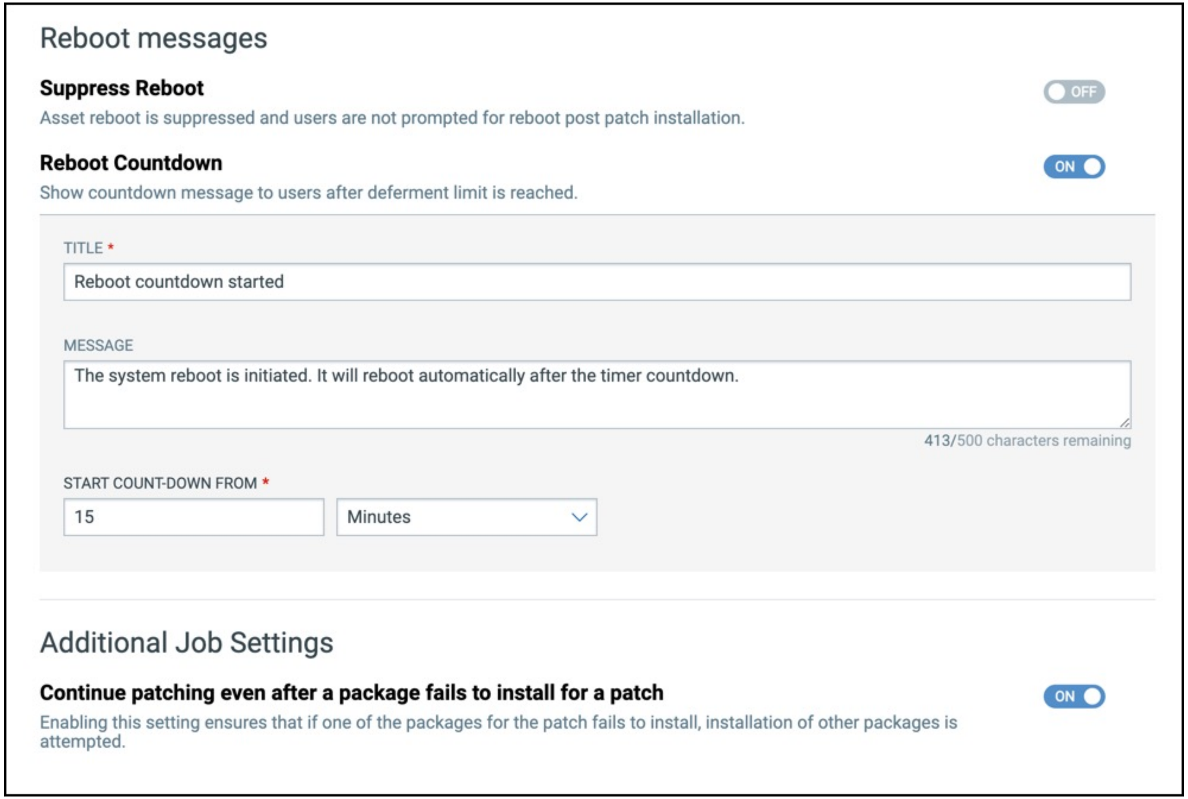
PM Processes & Executables



Name	9% CPU	46% Memory
Microsoft .NET Framework 4.7.2...	0%	1.1 MB
Microsoft Distributed Transacti...	0%	0.6 MB
Microsoft Malware Protection C...	0%	2.1 MB
Qualys Cloud Agent	0%	5.8 MB
Qualys Cloud Agent UI	0%	1.4 MB
RDP Clipboard Monitor	0%	1.7 MB
Runtime Broker	0%	3.2 MB
Search	0%	0.5 MB
Spooler SubSystem App	0%	1.6 MB

- When patching is active on a Windows host, patching messages and notifications are managed by the “Qualys Cloud Agent UI” process (QualysAgentUI.exe)
- ‘stdeploy.exe’ is the name of the patching executable.

Linux Communication Options



Reboot messages

Suppress Reboot

Asset reboot is suppressed and users are not prompted for reboot post patch installation.

Reboot Countdown

Show countdown message to users after deferment limit is reached.

TITLE *

Reboot countdown started

MESSAGE

The system reboot is initiated. It will reboot automatically after the timer countdown.

413/500 characters remaining

START COUNT-DOWN FROM *

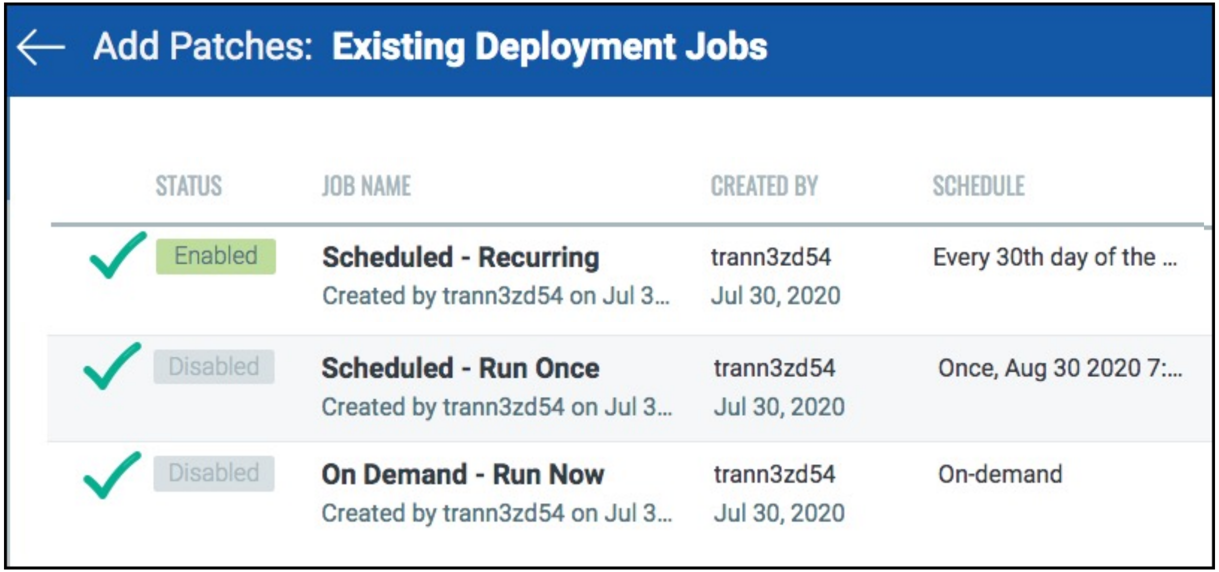
15 | Minutes

Additional Job Settings

Continue patching even after a package fails to install for a patch

Enabling this setting ensures that if one of the packages for the patch fails to install, installation of other packages is attempted.

Add to Existing Job?

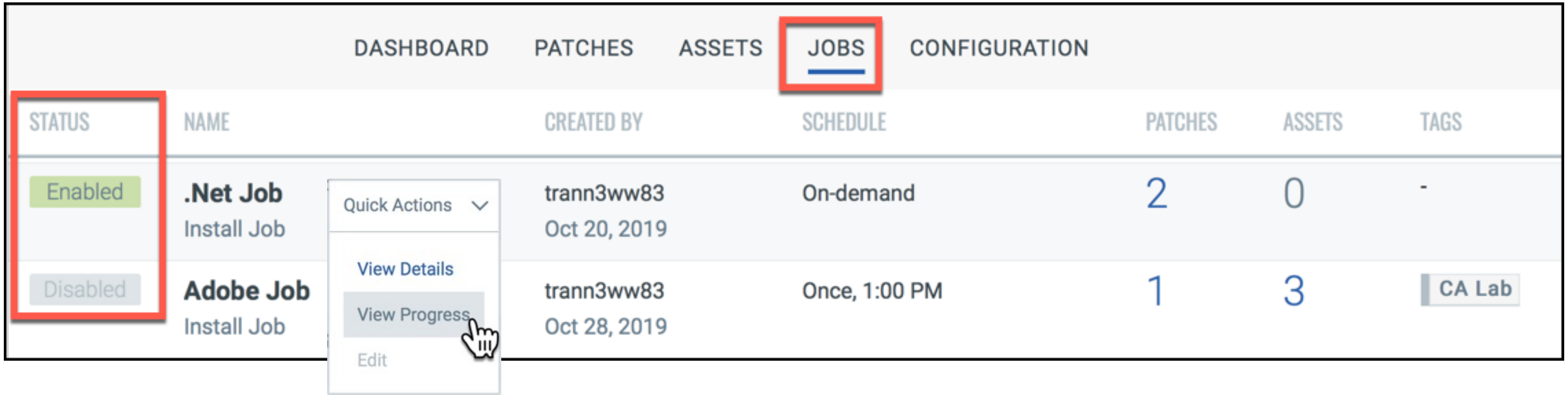


Add Patches: **Existing Deployment Jobs**

STATUS	JOB NAME	CREATED BY	SCHEDULE
✓ Enabled	**Scheduled - Recurring** Created by trann3zd54 on Jul 3...	trann3zd54 Jul 30, 2020	Every 30th day of the ...
✓ Disabled	**Scheduled - Run Once** Created by trann3zd54 on Jul 3...	trann3zd54 Jul 30, 2020	Once, Aug 30 2020 7:...
✓ Disabled	**On Demand - Run Now** Created by trann3zd54 on Jul 3...	trann3zd54 Jul 30, 2020	On-demand

- Patches and assets can be added to any deployment job, before it is enabled
- Patches and assets can be added to a “recurring” job, both before and after it is enabled.

Job Status

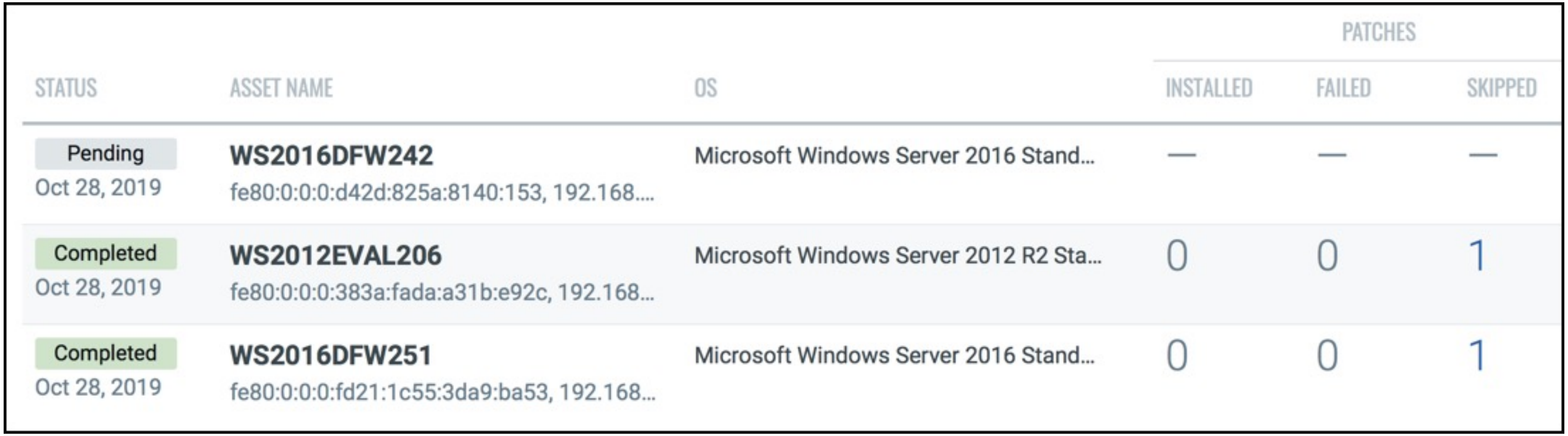


STATUS	NAME	CREATED BY	SCHEDULE	PATCHES	ASSETS	TAGS
Enabled	.Net Job Install Job	trann3ww83 Oct 20, 2019	On-demand	2	0	-
Disabled	Adobe Job Install Job	trann3ww83 Oct 28, 2019	Once, 1:00 PM	1	3	CA Lab

View Job Status:

- **Enabled** – Job is presently active.
- **Disabled** – Job is presently inactive.
- **Completed** – Job has completed.

View Job Progress



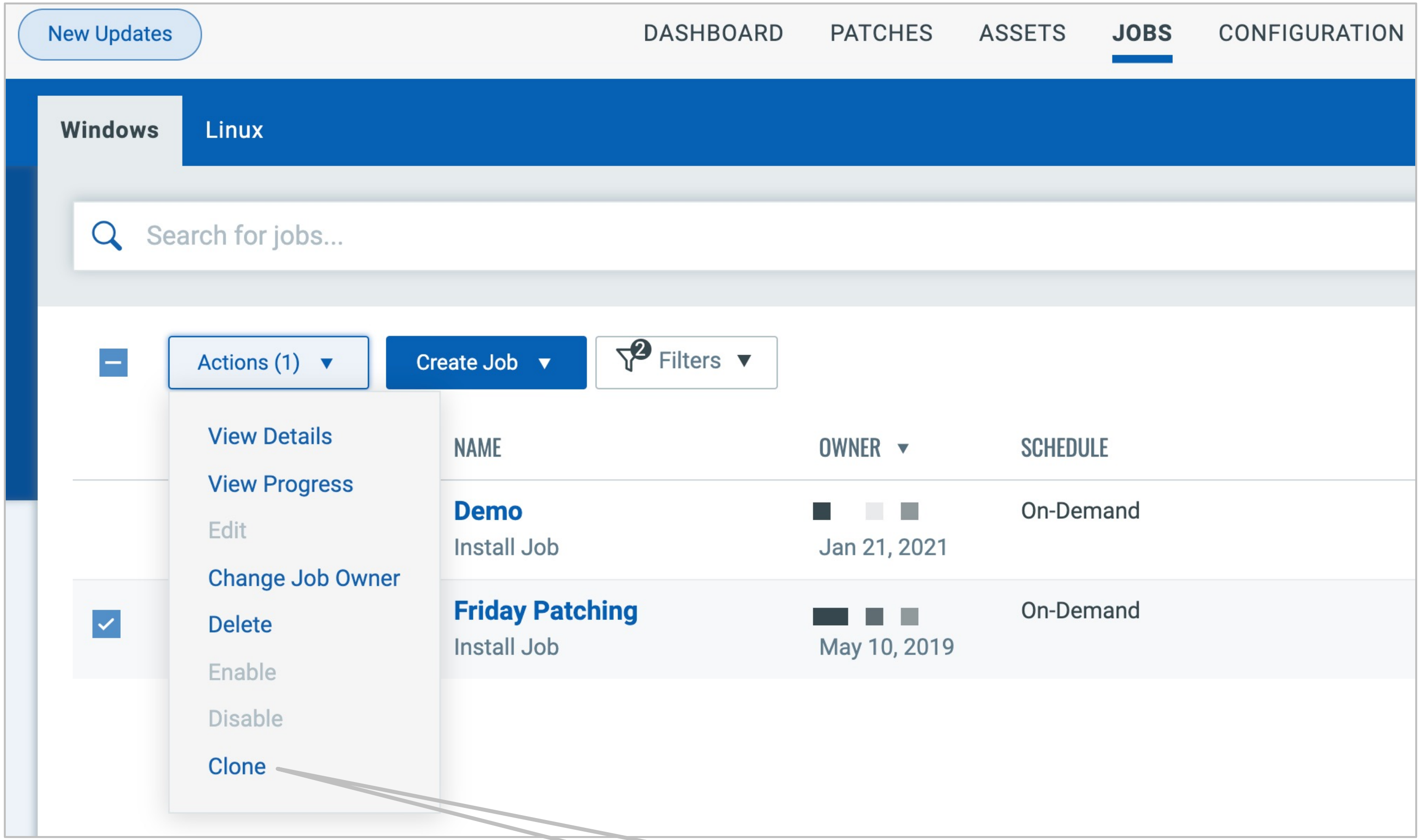
			PATCHES		
STATUS	ASSET NAME	OS	INSTALLED	FAILED	SKIPPED
Pending Oct 28, 2019	**WS2016DFW242** fe80:0:0:0:d42d:825a:8140:153, 192.168....	Microsoft Windows Server 2016 Stand...	—	—	—
Completed Oct 28, 2019	**WS2012EVAL206** fe80:0:0:0:383a:fada:a31b:e92c, 192.168...	Microsoft Windows Server 2012 R2 Sta...	0	0	1
Completed Oct 28, 2019	**WS2016DFW251** fe80:0:0:0:fd21:1c55:3da9:ba53, 192.168...	Microsoft Windows Server 2016 Stand...	0	0	1

Pending | Job Sent | Downloaded | Patching | Pendin ⏻ | Completed

Best Practices

- Use Asset Tags as targets for patch deployment jobs.
- Deploy patches to test hosts, first (create Asset Tags that distinguish between test and production assets).
- Once test deployments are verified, **clone the deployment job** and include production asset tags

Clone job

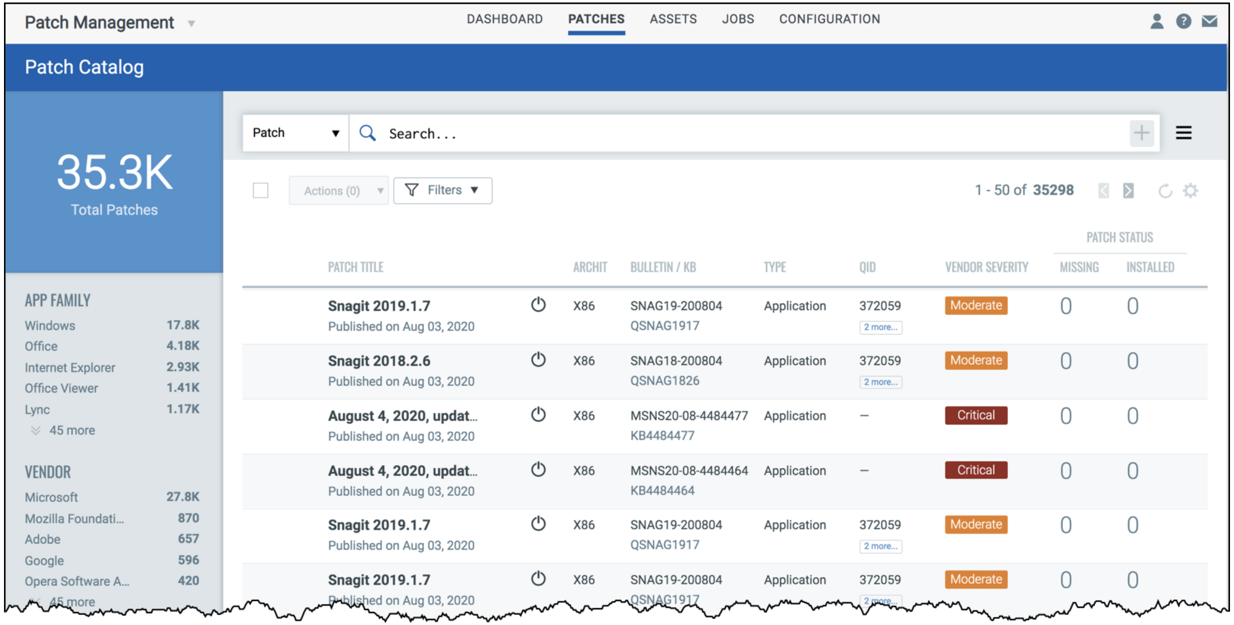


	NAME	OWNER ▼	SCHEDULE
	Demo Install Job	[redacted] Jan 21, 2021	On-Demand
☑	Friday Patching Install Job	[redacted] May 10, 2019	On-Demand

Clone an existing job

Patch Catalog

Patches



Patch Catalog

35.3K
Total Patches

APP FAMILY

Windows	17.8K
Office	4.18K
Internet Explorer	2.93K
Office Viewer	1.41K
Lync	1.17K
45 more	

VENDOR

Microsoft	27.8K
Mozilla Foundati...	870
Adobe	657
Google	596
Opera Software A...	420
45 more	

1 - 50 of **35298**

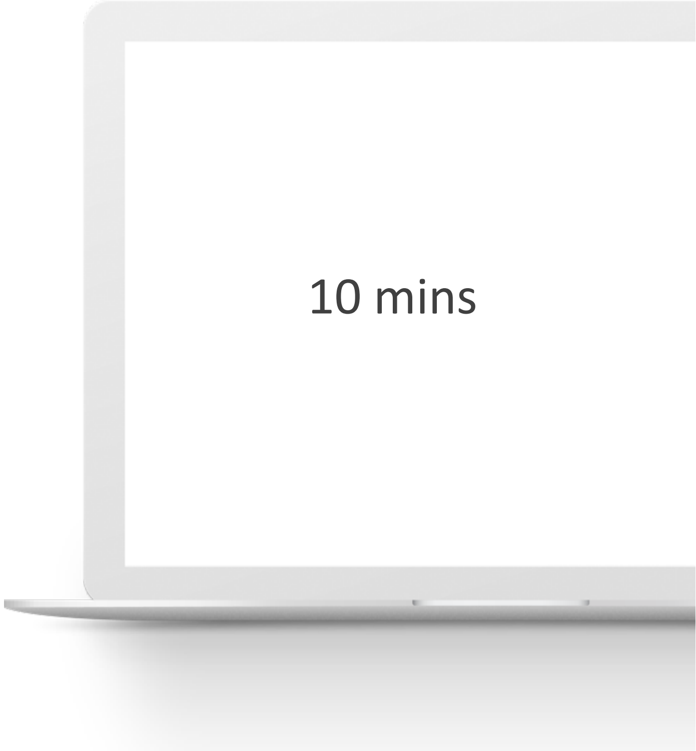
PATCH TITLE	ARCHIT	BULLETIN / KB	TYPE	QID	VENDOR SEVERITY	PATCH STATUS MISSING	 INSTALLED
Snagit 2019.1.7 Published on Aug 03, 2020	X86	SNAG19-200804 QSNAG1917	Application	372059 2 more...	Moderate	0	0
Snagit 2018.2.6 Published on Aug 03, 2020	X86	SNAG18-200804 QSNAG1826	Application	372059 2 more...	Moderate	0	0
August 4, 2020, updat... Published on Aug 03, 2020	X86	MSNS20-08-4484477 KB4484477	Application	–	Critical	0	0
August 4, 2020, updat... Published on Aug 03, 2020	X86	MSNS20-08-4484464 KB4484464	Application	–	Critical	0	0
Snagit 2019.1.7 Published on Aug 03, 2020	X86	SNAG19-200804 QSNAG1917	Application	372059 2 more...	Moderate	0	0
Snagit 2019.1.7 Published on Aug 03, 2020	X86	SNAG19-200804 QSNAG1917	Application	372059 2 more...	Moderate	0	0

- The Patch Catalog contains tens of thousands of OS and application patches.
- Presently, you can add up to 2000 patches to a single job.

Lab 15 : Patch Catalog

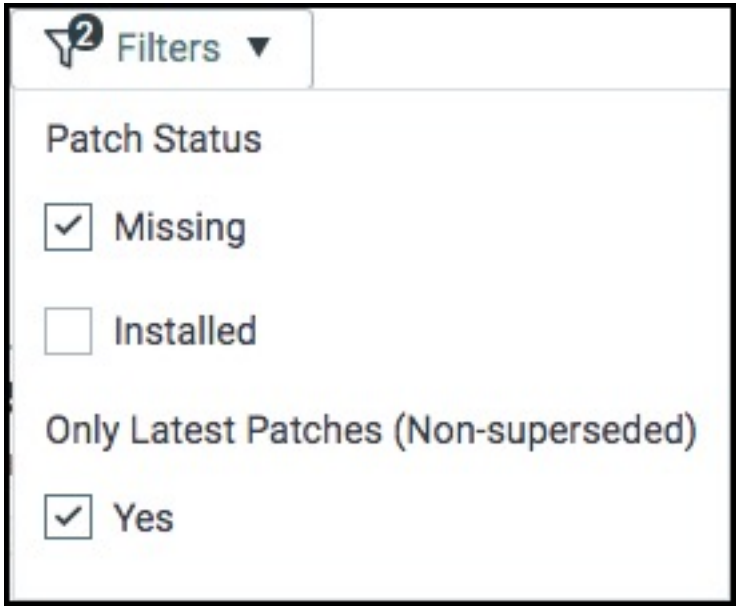
Please consult pages 58 to 61 in the lab tutorial supplement for details.

PLAY Tutorial begins on page 58.



10 mins

Catalog’s Default Display Filters



Patch Status

☑ Missing

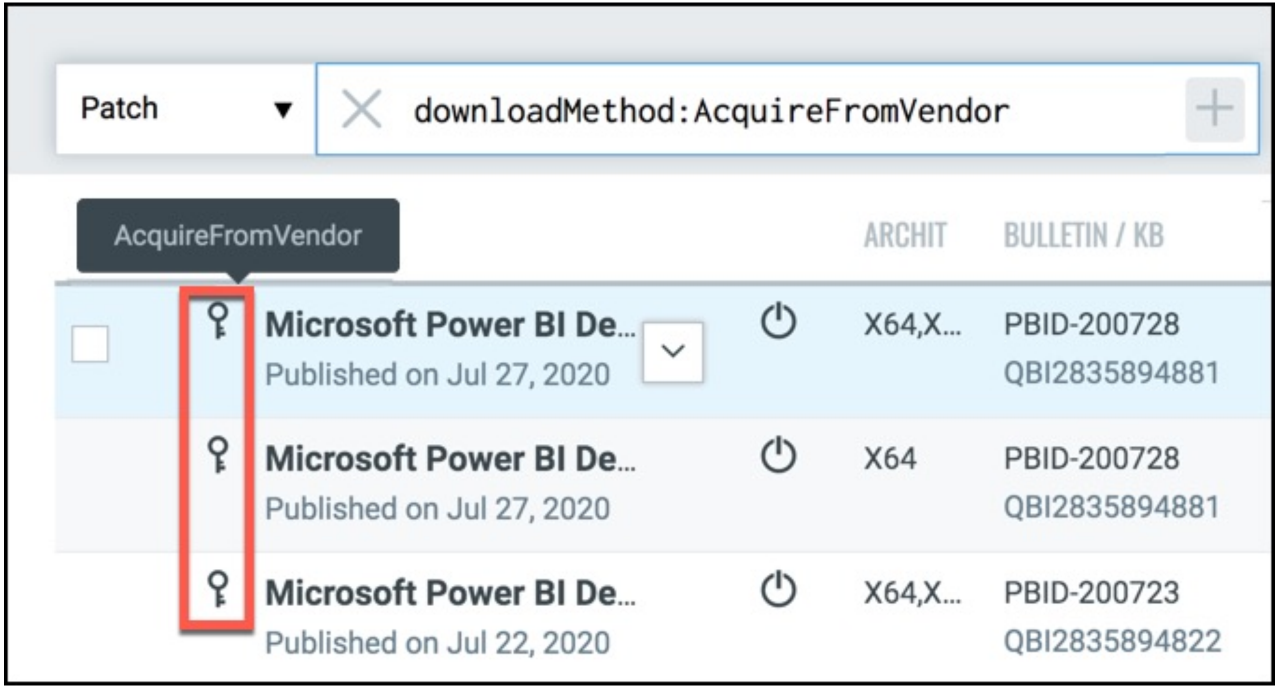
□ Installed

Only Latest Patches (Non-superseded)

☑ Yes

The default filters in the Patch Catalog, display patches that are missing and only the latest patches (non-superseded).

Acquire From Vendor



Patch ▾ downloadMethod:AcquireFromVendor

AcquireFromVendor

			ARCHIT	BULLETIN / KB
□	Microsoft Power BI De... Published on Jul 27, 2020	⏻	X64,X...	PBID-200728 QBI2835894881
	Microsoft Power BI De... Published on Jul 27, 2020	⏻	X64	PBID-200728 QBI2835894881
	Microsoft Power BI De... Published on Jul 22, 2020	⏻	X64,X...	PBID-200723 QBI2835894822

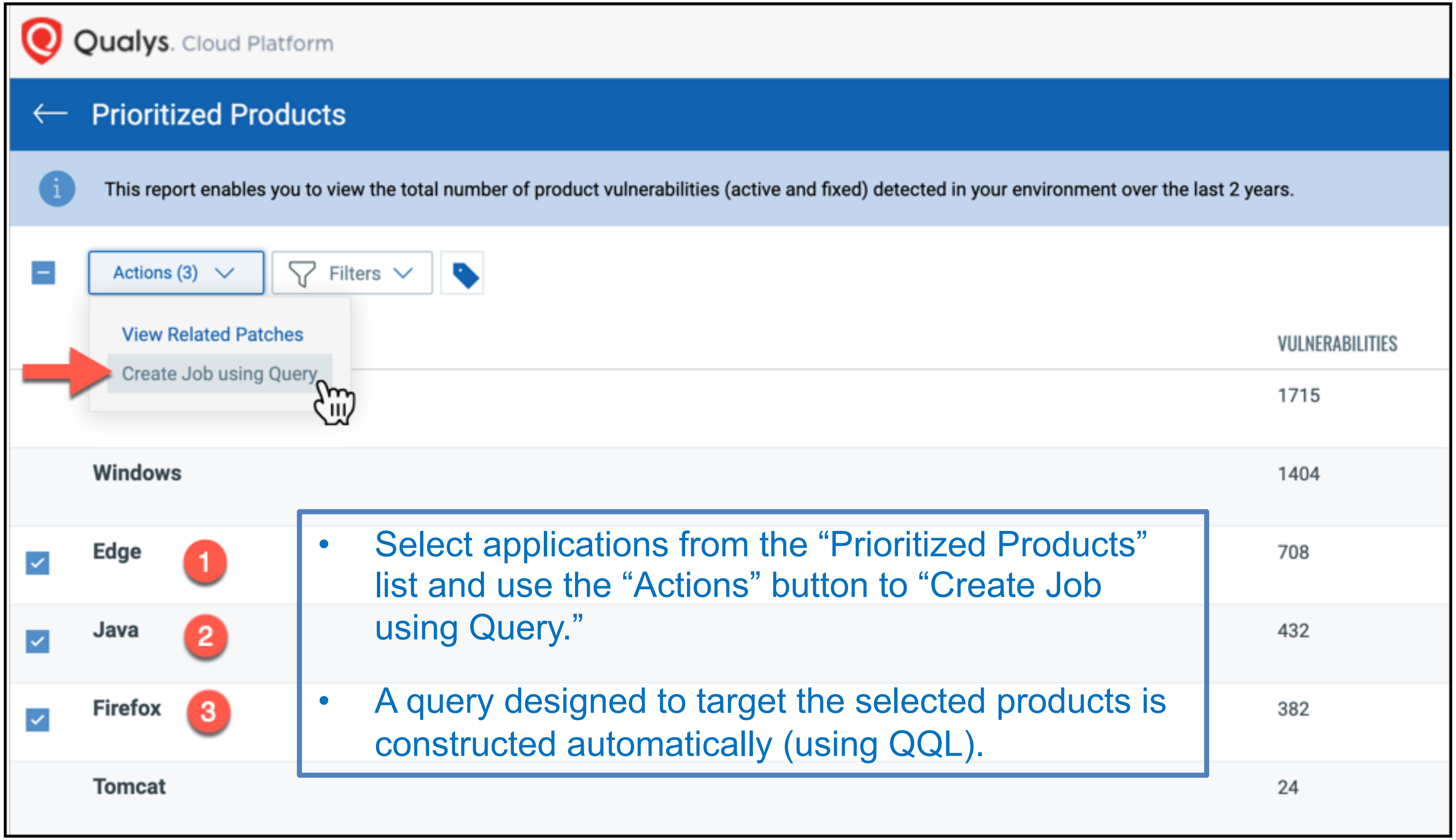
Patches identified with the “key-shaped” icon, cannot be downloaded by Qualys’ Cloud Agent.

Prioritized Products

Prioritized Products

- Focus on products in your environment that are important to patch on a regular basis
- Prioritizes products that have introduced the most vulnerabilities (over the last 2 years)
- Create a “zero-touch” patch job targeting products with most vulnerabilities
  1. Patches are selected using QQL
  2. Selected patches are included in recuring deployment jobs (daily, weekly, monthly)
- Click the “Prioritize Products” button from the Patch Catalog.

Create Job Using Query



Qualys. Cloud Platform

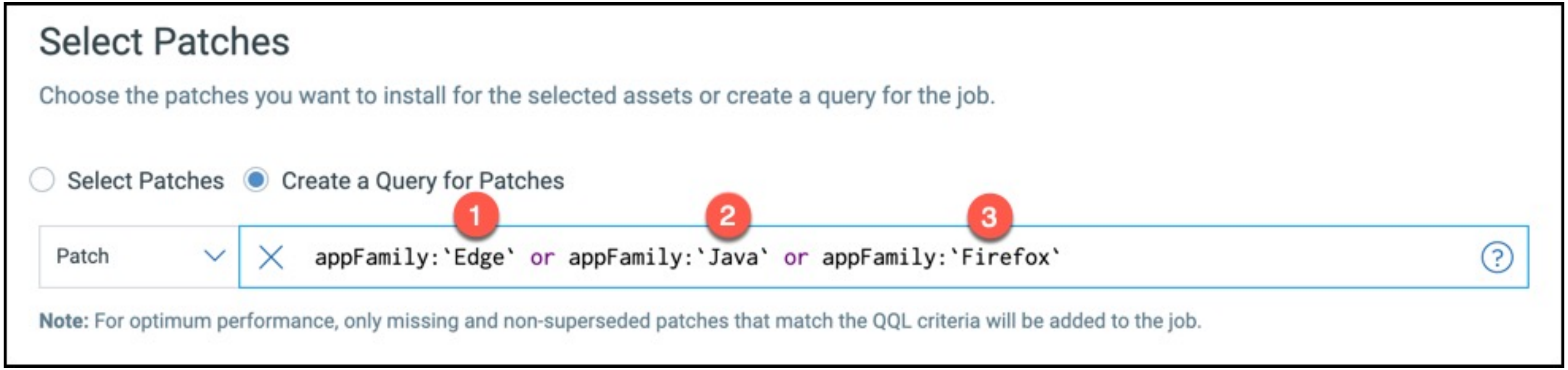
Prioritized Products

This report enables you to view the total number of product vulnerabilities (active and fixed) detected in your environment over the last 2 years.

	VULNERABILITIES
	1715
Windows	1404
☑ Edge 1	708
☑ Java 2	432
☑ Firefox 3	382
Tomcat	24

- Select applications from the “Prioritized Products” list and use the “Actions” button to “Create Job using Query.”
- A query designed to target the selected products is constructed automatically (using QQL).

Create a Query for Patches



Select Patches

Choose the patches you want to install for the selected assets or create a query for the job.

○ Select Patches ● Create a Query for Patches

Patch

```
appFamily:`Edge` or appFamily:`Java` or appFamily:`Firefox`
```

Note: For optimum performance, only missing and non-superseded patches that match the QQL criteria will be added to the job.

- The generated query condition(s) will specify the criteria for selecting patches each time the job runs:
  - daily
  - weekly
  - monthly

Course Resources

VMDR Certification Exam

https://gm1.geolearning.com/geonext/qualys/scheduledclassdetails4enroll.geo?&id=22511237827

VMDR Trial Account

https://www.qualys.com/forms/vmdr/

You will find the exam link and trial account link at the back of the VMDR Lab Tutorial Supplement.

Qualys®

Continuous Security

Thank You

training@qualys.com